Pages 1 - 192

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Before The Honorable Vince Chhabria, Judge

In Re: Facebook, Inc., Consumer Privacy User Profile Litigation	)	**No: 18-md-2843 VC**

San Francisco, California
Friday, February 1, 2019

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

For Plaintiffs:

Keller Rohrback, LLP
1201 3rd Avenue, Suite 3200
Seattle, WA 98101
BY: DEREK W. LOESER, ESQ.
CARI LAUFENBERG, ESQ.

Bleichmar Fonti & Auld, LLP
555 12th Street, Suite 1600
Oakland, CA 94607
BY: LESLEY E. WEAVER, ESQ.
JOSH SAMRA, ESQ.

For Facebook:

Gibson Dunn and Crutcher
200 Park Avenue
New York, NY 10166
BY: ORIN SNYDER, ESQ.

Gibson Dunn and Crutcher
555 Mission Street, Suite 3000
San Francisco, CA 94105
BY: JOSHUA LIPSHUTZ, ESQ.
KRISTIN LINSLEY, ESQ.
CHRISTOPHER LEACH, ESQ.

Reported By: Vicki Eastvold, RMR, CRR
Official Reporter

Friday - February 1, 2019 **10:34 a.m.**

P R O C E E D I N G S

---000---

THE CLERK: Your Honor, now calling for the record 18-md-2843 regarding Facebook, Incorporated, Consumer Privacy User Profile Litigation.

If parties could please come forward and state their appearances for the record.

MR. LOESER: Derek Loeser from Keller Rohrback for the plaintiffs, Your Honor.

THE COURT: Hello.

MS. WEAVER: Good morning, Leslie Weaver of Bleichmar, Fonti.

THE COURT: Good morning. Who else do you have with you? Maybe you could at least introduce them or -- either way.

MS. LAUFENBERG: Good morning, Your Honor. Cari Laufenberg for the plaintiffs.

THE COURT: Good morning.

MR. SAMRA: Good morning, Your Honor. Josh Samra for the plaintiffs.

THE COURT: Hi.

MR. SNYDER: Good morning. Orin Snyder for Facebook.

THE COURT: Good morning.

MR. LIPSHUTZ: Good morning, Your Honor. Joshua Lipshutz for Facebook.

THE COURT: Good morning.

MS. LINSLEY: Morning. Kristin Linsley also for Facebook.

THE COURT: Hello.

MR. LEACH: Morning, Your Honor. Christopher Leach for Facebook, too.

THE COURT: Hi. Okay. So we have a lot to talk about today. Why don't -- I guess why don't we start by talking about standing. And I feel there will be a fair bit of back and forth, so whoever's going to be talking about standing from either side, if you could come up.

And so maybe I'll start with you, Mr. Snyder, on, you know, the topic that I introduced in the order that I put out yesterday.

I have always understood the standing inquiry to involve an assumption that the plaintiff would win on the merits. And then you ask, well, if the plaintiffs would win on the merits -- assuming for the purposes of standing discussion the plaintiffs will win on the merits -- you know, were they injured? And was the injury fairly traceable to the conduct of the defendant? And can it be remedied?

In this case, depending on how you look at it, it seems like there could be a complete overlap between an aspect of the standing inquiry and the question whether the plaintiffs have stated claims on the merits, at least as they relate to the

privacy claims. Right? And that is the issue of consent. Right?

MR. SNYDER: Yes.

THE COURT: One way of looking at it is to say that there is no injury unless the private information was disseminated without the plaintiffs' consent. There's no injury for standing purposes. And that's, basically, the same inquiry as the one you would undertake to analyze Facebook's defense that they consented to our disclosure of this information.

On the other hand, you know -- to me, that's counterintuitive. Or at least as somebody who has, you know, went to law school and learned about standing in law school and litigated the issue of standing, you know, we're always taught that we're supposed to assume that the plaintiff is going to win on their claim when we're analyzing standing.

So maybe here I should be assuming for purposes of the standing inquiry that there was no consent. And I'm curious how you think -- I mean, you have this kind of very brief blurb in your opening brief that says: The first reason there's no standing is there was no consent. And you don't ever really circle back to that. And as I recall, you just cite -- you don't even cite, like, federal cases for that proposition.

So what is your support -- to the extent you continue to hold that position, what is your support for it? What is your

Article III support for it?

MR. SNYDER: Thank you, Judge. And we appreciate the question. Because even before we got your questions which clarified our thinking, frankly, we were talking about consent and how it functions on many levels, as Your Honor indicated, of the analysis.

And I think a threshold matter is that in order for there to be standing, you first have to demonstrate that there is at least an allegation of a facial violation of the statute that is plausible. And we believe that before you even get to the *Spokeo* analysis of what was Congress's judgment and --

THE COURT: But let me see if I can get -- sorry to interrupt but I just want to get kind of a direct answer to my question, then you can explain why you support that answer.

But you say that there has to be an allegation of a facial violation of the statute, or the tort, or whatever, that is plausible. And they'd have an allegation that Facebook disclosed sort of a bare allegation; but an allegation that Facebook disclosed this information to third-party apps and whatnot without my consent, right? And I gather what you're saying is that's not enough for standing purposes. For standing purposes they have to plausibly allege that there was no consent and that the allegations in their complaint actually suggest that there was consent.

MR. SNYDER: They have to plausibly allege that they

fall within the ambit of either the statute or the common law which they say gives rise to some injury. So even before --

THE COURT: So that includes consent.

MR. SNYDER: Yes.

THE COURT: So in other words, your answer to my threshold question is: Yes, the inquiry is exactly the same for standing as it is for the 12(b)(6) inquiry on the privacy claims.

MR. SNYDER: For sure. Because then when you get to the question of -- so as a threshold matter, number one, consent negates standing. Because there isn't even a plausible allegation that the statutes and laws apply.

THE COURT: Okay. So what -- well --

MR. SNYDER: Not plausible. Because they allege in paragraph 121 of the complaint that all their information was shared consistent with their privacy settings.

THE COURT: No, I understand. But what -- so what is your -- what is your case law -- your Article III case law for the point that consent negates standing?

MR. SNYDER: Well, I think that the case law we have is *Spokeo*, which holds clearly that you have to fall within the ambit of the statute at issue for there to even be an analysis of harm. In other words, even before you get to the harm analysis, our position is the consent negates standing because the plaintiffs, based on their own admissions in the complaint,

don't even fall within the ambit of the laws they're invoking. And so while that's a substantive defense --

THE COURT: Well, no, I don't -- I don't think that is a standing issue. I mean, that happens every day in courts across the land where people allege that they were injured and that certain conduct by the defendant injured them, and that that conduct violated X statute or Y, you know, common law tort. But, in fact, the conduct does not fall within the ambit of the statute or the common law tort. That doesn't mean they don't have standing. That means they failed to state a claim.

MR. SNYDER: Well, certainly the consent issue goes to harm. That is that every sharing of information under that -- well, let me go back to the threshold point because I don't want to quibble about it because the consent does negate standing as a matter of law under *Spokeo*, under *Eichenberger*, under all of the cases that define how you determine Article III standing post-*Spokeo*. So the fact that there's consent negates any expectation of privacy here in the meaning of whether it's SCA case law or whether it is state law privacy statutes or otherwise.

So as to your first question -- and we can get into *Eichenberger* because I think it fully supports our position -- there's no concrete privacy injury within the meaning of the standing jurisprudence when a user, as the plaintiffs admit here, authorizes friends to share their information, including

with apps. It's not private in the sense of our common law understanding of privacy law.

In fact, the sharing that occurred here is consistent with the decisions users make through their privacy settings. So stated another way, Facebook respects privacy -- the privacy of its users by honoring scrupulously, as the plaintiffs admit in paragraph 121, the choices they make through their privacy settings. And so to the extent their information gets to Kogan or gets even to the parties beyond Kogan, it's a function of user choice manifested through users' settings.

Once you have that consent, which is plain and clear and we believe as a matter of law enforceable against the plaintiffs, a person cannot be injured in fact by the sharing of information when the person consented to that very sharing the information.

What's remarkable about this case, Your Honor, is --

THE COURT: They could -- I mean, I don't think categorically that's correct.

MR. SNYDER: Well, not categorically. But then you look to *Spokeo* and *Eichenberger*, and it says what do you do? Well, in the Article III setting you first look to congressional judgment. And I guess if we look at the SCA, which I guess is their --

THE COURT: Well, we have the SCA. But we also have the California constitutional claim and --

MR. SNYDER: We do.

THE COURT: And you make this consent argument and you kind of apply it in the same way to all of those claims. And later we will talk about whether it's appropriate to do that or not. But for now, for assessing standing, I mean, show me where -- show me the language in *Spokeo*, for example, or *Eichenberger*, that stands for the proposition that consent negates standing in a case like this.

MR. SNYDER: I believe *Eichenberger* stands for a broader proposition, which is that you have to look to the context of the alleged harm to determine whether there's an injury in fact.

THE COURT: Okay. So show me the language in *Eichenberger* you're talking about.

MR. SNYDER: Well, in *Eichenberger*, of course -- I'll get to the language in one moment, but just to put it in context -- was about the Video Privacy Protection Act. And obviously, not about the SCA. It's a consumer protection statute. And what it did there, unlike the SCA, is it created a brand new right of privacy, a substantive right of privacy to protect consumers. And the Ninth Circuit explained this when it --

THE COURT: I don't think Ninth Circuit characterized it as a brand new right of privacy. Right?

MR. SNYDER: Well, it codifies -- this is the language

for the Ninth Circuit. It codified a context-specific extension of the substantive right of privacy. Namely --

THE COURT: Different than creating a brand new right of privacy.

MR. SNYDER: Well, a new category of information that is deemed protectable or protected by an act of Congress. In this instance, a substantive privacy interest in a consumer's video viewing history. And the court explained there that it had an analog in the common law, which was the tort of intrusion upon seclusion. Meaning, obviously, the things you do in the privacy of your home, unless you make them public, have an expectation of privacy.

THE COURT: So -- I'm sorry to interrupt, but I'm confused about one thing. Let's take a step back for a second and then we can get back into these cases.

You know, there's the issue of whether there's kind of automatic standing to bring a claim under the Stored Communications Act and the Video Privacy Protection Act. Sounds like you want to say that there's not, and there's a question about whether you fall within the ambit of the statute. That's fine.

But I want to ask you to put that aside for just a second.

MR. SNYDER: Yes.

THE COURT: Because I'm asking a broader question.

MR. SNYDER: Yes, Your Honor.

THE COURT: Sort of somewhat of a more abstract question that relates to standing for -- potentially for all the claims, not just the federal statutory claims. Okay?

So if it's easier, let's just take the, for now, the tort claim, the California tort claim and the California constitutional privacy claim, okay? So this is not an issue of Congress having created standing. The question is whether there's Article III standing.

I assume you would agree that a true invasion of a privacy interest, a true privacy injury, which you claim does not exist here, but a true privacy injury gives rise to Article III standing.

MR. SNYDER: Sure. Of course.

THE COURT: And so the -- you know, here they have alleged that their information was disclosed by Facebook without their consent, and they need to establish that to win on the merits of their claim. And the question I'm still struggling with, the question I'm still having a hard time understanding, is why do they need to do more than what they've done in the complaint to get standing?

MR. SNYDER: They do need to do more. I'll explain why. And what they've done is wholly inadequate under *Spokeo*.

THE COURT: Well, *Spokeo* is about whether Congress can statutorily confer standing, and I'm trying to get away from that.

MR. SNYDER: It's also about a requirement of a concrete *de facto*, real life injury, whether tangible or intangible. They're claiming here an intangible privacy injury; whether it's under the California constitution, whether it's intrusion on seclusion, whether it is any other flavor of state law, statutory law, privacy claim --

THE COURT: And you're saying that *Spokeo* and *Eichenberger* stand for the proposition that consent negates standing.

MR. SNYDER: No. They stand for the proposition that you need a real life actual injury, which requires that you look at the allegations of the complaint. And as pled, they plead themselves out of court because their allegations negate any plausible allegation of a legally protected privacy interest which is actionable under any statute. And the reason for that is clear.

They acknowledge, admit in a binding admission, that the information shared was consistent with their privacy settings.

THE COURT: I understand that argument. But what about the rule that you're supposed to assume that they're going to win on the merits for purposes of conducting your standing analysis?

MR. SNYDER: But, Your Honor, there has to be, under the case in controversy requirement of the United States constitution, a plausible allegation of injury. That is a

threshold determination for this Court before this Court can get to the merits. And there is no actual injury when they're claiming privacy-like injuries where the social media user, the named plaintiffs, shared information with their friends, just like a letter writer sends a letter to a friend, knowing, because they assented to it, that the recipient of that information -- in this case Kogan -- would not only get their information but you know that friends' information can be shared, too. So a friend knows that if they send something to a Facebook user, unless they --

THE COURT: I understand your argument about why they consented. I get that.

MR. SNYDER: But the consent negates, as a matter of law, as a matter of common sense, any plausible allegation of a privacy interest. How can there be a privacy interest, Your Honor, in information which the plaintiffs themselves acknowledge they freely and knowingly shared not only with their friends, but understood and assented to their friends sharing it with third-party apps? That's just what happened in this case.

THE COURT: I understand. But I'm asking -- the question I'm asking you that you're not answering is there is this rule that says you're supposed to assume that they are going to be able to win on their claims. One of the ways in which they would need to win is by establishing that there was

no consent. And so what I want to know is if you have a case that says, Hey, their failure to allege consent not only means that they fail to state a claim; their failure to allege consent also means that they fail to allege standing.

MR. SNYDER: I have cases, and I believe it is not only Supreme Court precedent but consistent precedent in the aftermath of *Spokeo*, whether it's Beck in the Fourth Circuit, whether it is the Ninth Circuit --

THE COURT: Which was the Fourth Circuit case?

MR. SNYDER: Beck was the Fourth Circuit case involving the theft of the -- the theft of the laptop.

THE COURT: Okay.

MR. SNYDER: Let me just get the -- Beck was the case that also ruled that the more time that passes the less likely there's going to be an injury.

THE COURT: Right.

MR. SNYDER: And that certainly is the case here. There was an encrypted laptop. Names, birth dates, last four number of social security, physical descriptor, 7,400 patients, and there was no intentional targeting by a thief, no credible risk of credit card theft.

And, of course, here, Your Honor --

THE COURT: But what does that have to do with the consent question that I'm asking?

MR. SNYDER: But what I'm saying, Your Honor, is that

you don't assume they're going to win. You assume the well-pleaded allegations in the complaint are true. And the well-pleaded allegations of this complaint do not plausibly allege any actual harm, any *de facto* injury, any real world consequence that caused them injury.

And under our Article III jurisprudence, that's lights out for them. And you assume they will win only for redress-ability purposes, not injury purposes. I'm not aware of any case law, Your Honor, that says that any analysis of Article III dispenses with the threshold determination of: Have they plausibly alleged harm? And here, how can they allege harm, Your Honor, when they admit --

THE COURT: I understand. I understand.

MR. SNYDER: And so I don't think this is a close question, Your Honor.

THE COURT: Let me ask you about -- so, what would be the consequences of a conclusion that there is no -- that they haven't adequately alleged standing? I mean --

MR. SNYDER: Dismissal of the case with prejudice. Because --

THE COURT: No. It would be dismissal of the case under Rule 12(b)(1) which is inherently without prejudice, which I assume means they could, at least for the state law privacy claims, they could go to state court to assert them. Right?

MR. SNYDER: If they can plausibly assert them in a state court. In fact, there are plaintiffs in state court now alleging certain privacy wrongs and that will be adjudicated in the state court system.

THE COURT: So your suggestion is that I dismiss these claims and let Judge Buchwald handle them all.

MR. SNYDER: No. I'm suggesting that the Article II -- let me just say something that sounds dramatic, but it's intended to be, hopefully, instructive of our argument.

The reason, of course, Article III is the critical rule of -- sort of the gating question in federal cases is, of course, to protect the separation of powers and ensure that this Court, and other Article III courts, aren't wading into issues where there is no actual harm to these plaintiffs. We've made that point.

And, Your Honor, it is particularly important in this case because we acknowledge that the issues raised in the complaint here raise important public policy issues that are being debated in the halls of Congress, that regulators are grappling with. And that's precisely where those questions belong.

This complaint does not allege a single plausible injury. It does allege, in a broadside against Facebook, a lot of concerns they have about the Facebook platform. And what they're really complaining about, Your Honor, in this complaint is that they don't like the rules of the road on Facebook.

They have a lot of options for redress in that event. They can petition Facebook to change the rules. They can turn off Facebook and never use it. They can petition their Congress people to pass laws.

But what they can't do is come into this Court and say that their privacy rights were injured when they're participating in a social media platform, the very premise of which is the sharing of information. And if you look at the -- all of the common law --

THE COURT: Well, wait a minute. Hold on a second. I mean, what you seem to be saying there is that the fact that people share information with their Facebook friends means they have no expectation of privacy in that information.

MR. SNYDER: Absolutely not. What I'm saying is that Facebook --

THE COURT: But that is what you just said. You just said that they're complaining about their privacy. They're complaining about invasion of privacy when they are sharing information with their friends.

MR. SNYDER: Sharing information with their friends in accordance, Your Honor, consistent, with their manifested intent. And let me be clear about that.

Facebook respects all of its users' privacy. It honors the decisions that its users make through their privacy settings. To the extent user information makes its way to

third parties, as happened here, that is a function of user choice manifested through their settings.

THE COURT: Okay. And we'll talk a little bit more about that in a second. But I want to talk to the plaintiffs about the standing issue.

MR. SNYDER: May I just make one more point, Your Honor?

THE COURT: Sure. But these are very sort of high-level points that are pretty obvious from the briefs, so I'm trying to get into the nitty-gritty.

MR. SNYDER: Well, the nitty-gritty, Your Honor, is the threshold harm requirement as a matter of law is absent from this complaint. To the contrary the binding admissions in this complaint are clear.

THE COURT: I understand that. You've said that. Okay. So let me hear from the plaintiffs.

And, first, let me ask you what is your position on sort of whether the standing inquiry and the merits inquiry completely overlaps when it comes to the issue of consent.

MR. LOESER: Our position is that it does not overlap. And I want to --

THE COURT: What's your support -- I'm happy to have you explain it, but before I forget. What is your support for the proposition that it doesn't overlap? Do you have examples of cases where courts have said, no, there's -- you know, this

issue of consent in a privacy case is not for standing. It's for the merits.

MR. LOESER: Yes. We have cases. And I just want to make it clear so you know what question we're answering. This is really question -- second question and the third part. And that has to do with whether these issues that you've raised go to 12(b)(6) merits issue or standing issue, and whether those are two distinct analyses.

The first case I would point Your Honor to is ***Maya v. Centex***, 658 F.3rd 1060. It's a Ninth Circuit case from 2011 where the Ninth Circuit stated: In determining whether plaintiff states a claim under 12(b)(6), the court necessarily assesses the merits of plaintiff's case. But the threshold question of whether plaintiff has standing and the court has jurisdiction is distinct from the merits of its claim. Rather, the jurisdictional question of standing precedes and does not require analysis of the merits.

Another case, Your Honor, that I think is quite helpful on this *In Re: Vizio Consumer Privacy Litigation*, 238 F.Supp.3d 1204, which is a case out of the Central District of California. And at page 1216 of that case, in responding to a merits-based attack on whether the plaintiff had standing, the court wrote: But this argument improperly conflates the merits of plaintiffs' claims with their standing to bring suit. Taken to its logical conclusion, defendant's argument absurdly

implies that a court could never enter judgment against a plaintiff on a VPPA claim if it found that the disclosed information was not within the statutory definition of "personally identifiable information." Instead, it would have to remand or dismiss the action for lack of jurisdiction.

And I think that really does drill down on the heart of what you're asking.

In *Eichenberger*, for example, it's another case that --

THE COURT: But isn't it a little -- I'm sorry. Go ahead. Talk about that case then I'll ask my question.

MS. WEAVER: Thank you, Your Honor. In *Eichenberger* the court addressed the standing issue determining -- accepting the plaintiff's allegations that there was a violation of the VPPA, accepting that there was standing based upon congressional determination.

And then in the second half of the opinion the court addressed whether in fact the information that was identified qualified as personally identifiable information. The court did not dismiss for lack of standing because of the failure, in the court's view, to allege appropriately personally identifiable information. Instead, the court found standing and then assessed something which was not in dispute.

THE COURT: And I think the question here is, you know -- I don't think there's any -- they may disagree, but I don't think there's any serious argument that the general rule when

you're looking at standing is you're supposed to assume that they win on the merits and you're supposed to conduct the standing inquiry as sort of a precursor to diving into the merits. I think that's the general rule.

And I guess the question is: Is this one of those weird cases where there's an exception to it because the inquiry is the same? In other words, because of the nature of privacy violations, right? The nature of a privacy violation is that your privacy is not violated if -- you know, the injury that you're asserting, one of the injuries you're asserting, is a privacy violation. There's no privacy violation if you consented to that information being disseminated. And, therefore, it seems to me there's no privacy injury if you've consented to that information being disseminated.

And so maybe this is one of those strange cases where you ask that question at the standing threshold, and it's the exact same question that you ask when you're analyzing the defendant's consent defense to your claim on the merits.

So I'll ask you. The ***Maya*** case and the ***Vizio*** case, I will admit to you that I haven't read those cases yet. But do they talk about consent to the dissemination of information? Because that's really, I think, the issue that we're talking about here.

MR. LOESER: Yeah. And those cases do not -- the issue of consent was not the particular factual challenge that

was being made in those cases.

But I have two case ways to answer your question that I think both --

THE COURT: Before you answer it, let me just give you one other case that I want to make sure you're aware of. And that is -- I read last night. I'm sorry I didn't put it in the order, but I read it after I put the order out.

This is an Eighth Circuit case, if I recall correctly, called *American Farm Bureau Federation versus the EPA*. And it's from 2016. And it seems to get right at the heart of this in some ways. It says -- you know, the Eighth Circuit said, well, the district court -- and it was an issue about disclosure of information without consent. And the Eighth Circuit said, well, the district court erred in dismissing the case on standing grounds because it seemed like what the district court was really doing was prejudging the merits. And you need to assume for the sake of argument in the standing inquiry that the plaintiff is going to win on the merits. So the district court erred in dismissing on 12(b)(1) grounds.

And the court went on to explain why the plaintiff -- and that's sort of supportive -- what I've said so far about the case is supportive of your point. But then the court went on to analyze why the plaintiff had adequately alleged standing in that case. Why the plaintiff had adequately alleged a privacy injury in that case. And actually it was in the context of

summary judgment, but for purposes of our discussion I think that's neither here nor there.

It was undisputed on the motions for summary judgment that the agency has released, or will release, personal information of association members without their consent as part of its response to the FOIA requests. That is sufficient to establish a concrete and particularized injury in fact; the nonconsensual dissemination of personal information.

So in that part of the court's discussion, it makes it seem like in a context like this where lack of consent is part of the claim it will be a completely overlap between that and the standing inquiry. And so that's the one case that we found so far that touches on this issue of consent in a privacy case and whether that's relevant to standing.

Have you identified any others, yet?

MR. LOESER: There's a series of cases that I'll identify for Your Honor. And the reason why they matter -- first of all, I don't think that there's something so inherently different about these privacy claims. Consent is a defense. And it's -- courts frequently and constantly are evaluating on a 12(b)(6) whether a defense is demonstrated as a matter of law where there's a factual dispute about a defense. And I'll have to think more about other types of claims where a defendant would assert a defense that would undermine standing. I'm sure there are dozens.

THE COURT: A consent defense, in particular, I mean --

MR. LOESER: Right. For a variety of different claims. Not just for privacy violations. For theft. You know, conversion. All kinds of things.

THE COURT: Trespass, maybe. Something like that.

MR. LOESER: Yeah. Those would be a defense. But the standing analysis would not attempt to determine the merits of that defense. Instead, the standing analysis would look for an identified, concrete and particularized --

THE COURT: Yeah, but in the trespass example, I mean, if I allege -- if I file a lawsuit -- I don't know if you -- I've never seen a trespass claim in my five years here.

MR. LOESER: We'll add one against Facebook.

THE COURT: But, you know, let's say it's a diversity case, or whatever, and there's a trespass claim. And the allegations in the complaint indicate that there was consent. I know you disagree that the allegations in your complaint indicate that there was consent. And we will get to that, I promise.

But if the allegations in the complaint indicate consent, then I would think that it might be -- surely you would dismiss that on 12(b)(6) grounds, but before you even got to 12(b)(6) I think you might consider whether there was any injury since you, after all, consented to their being on the property.

Now, there might be an injury if they went on your property and then inflicted some other injury while they were on your property. But if it was a pure trespass claim, which I think is analogous to this, I would think that a court might say: Hey, there was no injury here. Or, you haven't adequately alleged injury because the complaint indicates that you consented to this person coming onto your property.

MR. LOESER: Yeah, I think the difficulty with your construct and with the question is that it only works if the factual issue that you're talking about is not in dispute. And what I hear Your Honor saying is that if there is really truly no dispute about this, does this mean that you can address this on standing as opposed to on merits? And I think the problem here is that that's not the case. It's not even close to the case.

THE COURT: Okay. And I promise we'll get to talk about that. But my question now -- or, another way of asking the question that I've been asking -- is if you conclude that there is standing, does that automatically mean that you have concluded that the plaintiffs have stated a claim? Or at least alleged enough to overcome their consent defense on 12(b)(6)?

Is that automatic? Because if your answer to that is yes, then what you're saying is the inquiry is the same on the standing -- on 12(b)(1) as it is on 12(b)(6).

MR. LOESER: Well, I'm going to try to be cute, which

would be that it depends how you made that determination on standing. I think that you're right, it's the other side of the coin. If in your standing analysis you carefully examine on, like, a factual matter, which you would have to do on this case on the consent issue, whether consent is appropriately pled, then you've engaged in a 12(b)(6) analysis and your conclusion would be equally --

THE COURT: But you're saying that I shouldn't do that.

MR. LOESER: I'm saying that the case law, including Ninth Circuit case law, would suggest that you shouldn't do that.

THE COURT: Well, but what you just said a second ago was if there is a factual -- if it's not clear from the allegations whether there was consent or not, or if you can't establish definitively from the allegations that there was consent, then you can't kick it out on standing grounds.

So is the converse true? That if I can definitively determine that there was consent based on the allegations I can kick it out on standing grounds? That's really the question.

MR. LOESER: And again, the hard thing about that is I've never seen a case like that. The case law that we look at draws this line between the analysis you do on standing and the analysis you do when you're evaluating the merits on 12(b)(6).

And so I don't really have an answer on whether it's

possible. I've never seen it in any case law, and it's not what exists here. I get your point. I get that you can't have your cake and eat it, too. If it's different, it's different on both. If you rule on standing, you probably wouldn't welcome my telling you that since you said standing exists then we survive the 12(b)(6).

On the other hand, I do think that the practical answer is if in your evaluation of standing you are evaluating this factual question of whether there's consent, then I think it is the same analysis and that's why it would --

I also think that's probably why in the defendant's brief when they go into this issue for the second time when discussing the claims they say, like we said before, Your Honor, there is no standing, therefore there's no injury.

THE COURT: Well, how could you -- I mean, given that the default setting for somebody who signs up for Facebook is that they share all their stuff with the public, how could you possibly get past a motion to dismiss, regardless -- whether it's 12(b)(1) or 12(b)(6), how could you possibly get past a motion to dismiss without alleging that the plaintiffs switched from the default settings?

MR. LOESER: So that is --

THE COURT: I know it's potentially something that could easily be fixed. But nonetheless, you don't have the allegations in your complaint.

MR. LOESER: Yeah. And I'm going to put the question back to you in exactly the way that it was posed to us. Because whoever wrote these questions, I think they need a very specific answer to these very specific questions. And that question you just asked is really the first question. Which is: Does it matter that plaintiffs have failed to allege that they switched from the default "public" setting to the "friends only" setting. That's effectively what you're asking.

And it doesn't matter, and here's why. And there's several reasons it doesn't matter and why we would survive a motion to dismiss.

And the first is that there is information that Facebook was not authorized to share even if the plaintiffs' settings are left on the default "public" setting. I'm putting aside the conversation we need to have about default "public" settings, which I think is a real issue in the case as to what Facebook was trying to accomplish and how clear they were being.

Every plaintiff in this case has alleged that they use Facebook Messenger. Facebook Messenger is a private communication. It's --

THE COURT: But there's no reason to believe that -- I don't know if we really want to go down the Facebook Messenger rabbit hole here because I don't think there's any reason to believe that the content of their communications in Facebook

Messenger were intercepted or disclosed, at least based on the allegations that are currently in the complaint.

MR. LOESER: I believe that there are reasons to believe that and that is among the information that was disclosed. And we can search for the paragraphs in the complaint and we should make sure we give them to you. But that is an issue in this case. These were private communications and they were disclosed. They were disclosed -- some of the Kogan, Cambridge Analytica, information --

THE COURT: But no reason to believe that it was for these plaintiffs. Because you allege that it was only like, what? 1,500 -- the content of 1,500 of the -- messages sent by like 1,500 Facebook users?

MR. LOESER: Based on the discovery responses we got that was the level of detail that we were provided. They could, of course, look up who these people are and tell us. But the complaint does allege Facebook Messenger is among the information that was disclosed.

THE COURT: Other than Facebook Messenger, what type of information was Facebook not allowed to disclose even if the privacy setting had not been changed from "public" to "friends only"?

MR. LOESER: Well, there was all of the sharing that wasn't affected in any way by the privacy settings. For example, they never told anyone that they were sharing all this

information with dozens of business partners. The complaint alleges that they did that.

THE COURT: Right. But if you set your Facebook privacy settings for your information to be shared with the world, then it's difficult to understand how you didn't -- how you have -- how you could have a privacy claim when Facebook provides some of that same information that you consented to disclosure -- that you set for disclosure to the world to particular recipients.

I thought what you were going to say is that there is some category of information connected to your Facebook account that even when you set your settings to -- even when you keep it on the default setting of "public," that information is not disclosed to the public, but Facebook is disclosing that information to third-party apps.

MR. LOESER: Well, let me make sure I tick through all these things. There is other information that -- Facebook collects information, they make inferences and determinations and things. And our allegation is that information is improperly shared.

THE COURT: Well, what's the information that is -- when you put your privacy setting at "public," or when you leave it on the default setting of "share my stuff with the public," what is the information that the public nonetheless does not have access to that you allege Facebook shares with

third-party apps?

MR. LOESER: Well, it's the Messenger information -- Messenger information -- and I think I can make this shorter. We are not alleging that information that was designated as "public" that was shared is the basis of a privacy claim. Public information shared is not the basis of our privacy claim.

I think the problem with your question is -- let me go back --

THE COURT: But you have not alleged that the plaintiffs switched from Facebook's default setting to limit the sharing of information to "friends only."

MR. LOESER: And here's why that doesn't matter. For the majority of the class period, the default setting was "friends only," not "public." For 2007 through 2010, and 2014 to 2018, the default was "friends only."

So your question assumes facts that are contrary to what happened, and what's evident in the materials Facebook itself has presented, and what's alleged in the complaint. So for those people, it's a hypothetical and it doesn't apply. For most of the class period for most of the people the default wasn't "public."

The only period of time when the default was "public" was April 2010 through May 2014. And this should sound very factual to you, Your Honor, because --

THE COURT: Sorry. What were those dates again?

MR. LOESER: April 2010 to May 2014. This is a very factual conversation, and I think it indicates why we're kind of jumping ahead to what is really is typically the type of conversation we'd be having at summary judgment.

But at this 2010-2014 time period, the question still doesn't mean the complaint doesn't survive, because 13 of the plaintiffs allege that for the entirety of the class period their privacy settings were set to "nonpublic, friends only."

The complaint also alleges that --

THE COURT: Sorry. Say that one more time.

MR. LOESER: So for 13 plaintiffs in the complaint -- and we can tell you who they are -- for the entirety of the class period their settings were set to "nonpublic, friends only."

THE COURT: Show me an example of that. I want to just look at the language in the complaint.

MR. LOESER: I don't have a paragraph cite in my outline, but we can dig one up.

And while we're looking for that, Your Honor, we also have allegations in the complaint that people changed their settings over time.

THE COURT: Okay. But let's just look at a concrete example of what's alleged in the complaint in that regard.

MR. LOESER: Would you like me to make another point

while we're digging for that, Your Honor?

THE COURT: No, no. We can wait.

(Pause.)

MR. LOESER: While we're waiting, we do have a presentation that has some interesting slides in it. Did we hand one up?

THE COURT: I don't have it, but feel free to hand --

MR. LOESER: While we're killing time --

THE COURT: Do you have an extra one for my law clerk?

(Pause.)

MR. LOESER: The mystery is unraveling, Your Honor. Paragraphs 21 through 88, we allege that the plaintiffs intended for the information to be private.

THE COURT: Well, wait a minute.

MR. LOESER: I'll give you the rest of the answer. In conversations with our clients, the contents of which I probably shouldn't talk about, we have developed more information. So this would be something in your question about what to amend. We could specifically allege who those 13 people are.

THE COURT: So what can you tell me about that now? About what you would allege? Simply that they -- that 13 of the plaintiffs changed -- switched from the default "share with public" setting to "share with friends only"?

MR. LOESER: Well, for much of the class period that

wasn't the default.

THE COURT: And where is that in the complaint? That for much in the class period it wasn't the default?

MR. LOESER: I think the complaint goes through every single one of these --

THE COURT: Show me where it is in the complaint.

MS. WEAVER: Those allegations aren't in the complaint with regard to the default settings. Because we had, frankly, Your Honor, assumed that the content -- the entire thrust of our complaint was premised on the concept that the information that the plaintiffs were --

I'm sorry. Leslie Weaver on behalf of the plaintiffs.

So allegations that we would seek leave to amend would include these allegations about the default settings, and then only this four-year period being where it was "public" only. We could also amend to add claims for these 13 plaintiffs. We are still in the process of talking with people so we don't have complete responses for everybody. But at least for those 13 my understanding is that they have adopted the default setting "friends only" throughout their usage. I don't know how that overlaps with the class period specifically.

THE COURT: Okay.

MS. WEAVER: There's another point I just wanted to make about what is in the complaint.

Facebook Messenger is not just -- it's not even analogous

to email, I would say, because it's within an environment where you already have protected communications and you're defining your circle of acquaintance. And so when you go to Messenger, somebody, you can send content, you can send photos, you can send --

THE COURT: No, I get all that. My only beef with Facebook Messenger is that as it relates, I guess, to standing, it's -- you know, there's just -- I'm not sure we have enough to believe that the content of any of the plaintiffs' messages were disclosed by Facebook to third parties.

MS. WEAVER: That we do have. And if you turn in your presentation -- we actually have a slide that is cited in the complaint.

THE COURT: I'd be more interested looking directly at the complaint.

MS. WEAVER: Sure. Sorry. Paragraph 145.

THE COURT: Okay. Hold on.

MS. WEAVER: And this --

THE COURT: Wait. Hold on. Real quick let me get to it.

MR. LOESER: Your Honor, we're going to occupy both of these podiums for awhile.

THE COURT: But this doesn't talk -- the question I was asking about -- I've looked at this chart.

MS. WEAVER: Right.

THE COURT: But the question I was asking about was these particular plaintiffs. Right?

MS. WEAVER: Oh, I see. Whether these particular plaintiffs --

THE COURT: But I think it's --

MS. WEAVER: Well --

THE COURT: I think it's pretty easy to assume -- it's more than assume -- that plaintiffs' Facebook information was taken from their friends, and maybe some of them from themselves, by Kogan, and then given to Cambridge Analytica. I think it's probably also safe to assume that a lot of -- that their personal information was acquired from Facebook by other third-party apps. But I'm not sure that it's safe to assume that the contents of the plaintiffs' messages through the instant messaging system were acquired by Kogan or by anyone else.

MS. WEAVER: I can explain that. And we do allege that. And I believe that to be true.

THE COURT: Okay. Show me where you allege it.

MS. WEAVER: And this is very interesting because it's going to return to the sentence that defendants keep citing in paragraphs 121 and 122.

Those paragraphs explain how Graph API, Version 1.0, operates. That is too many words to explain that it is the platform that Facebook built so that app developers could

syphon off the content and information of the users. And how it worked -- and what we meant to be describing in this page (indicating) --

THE COURT: Well, I don't want to know what you meant to be describing. I want to know what you actually described.

MS. WEAVER: What we're describing here --

THE COURT: Because let me just say. I mean, look. Even if this complaint gets dismissed or even if, you know, significant portions of the complaint gets dismissed, it's going to be with leave to amend, right? Almost certainly. There may be an exception of a couple claims. But, so really my job here is not to ask whether this lawsuit is going to be thrown out forever. My job here is almost exclusively merely to ask whether this particular version of the complaint is inadequate and whether you need to take a shot at going back and beefing up your complaint.

So I want to know what you've actually alleged.

MS. WEAVER: I understand.

THE COURT: Not what you talked to your clients about, or whatever.

MS. WEAVER: Right. What we actually allege here, starting in paragraph 120, is how API, Version 1.0, worked. And we wrote this, actually, in consultation with our experts.

So, this explains that a user installs an app and then allows an app to get an access token from Facebook. That's

like a temporary password that -- and I'm no technical expert myself, but this is what it says here.

The user will then select which categories they want to be downloaded onto the app. And then those privacy settings --

THE COURT: When you talk about the user -- okay -- sorry. Go ahead. I understand.

MS. WEAVER: So the sentence here that it says "as long as the request complies with the users and friends privacy settings," is actually only very, very narrow and specific to how API-1 worked. It was never a categorical -- we obviously don't think the privacy settings were complied with. This is just how API-1 functions.

And so if you combine that with the allegations in paragraph 145, which are the admissions of what Kogan got, Kogan got messages of individuals from users who downloaded the app.

THE COURT: But only -- okay. Let me see. Let me look at paragraph 145.

So where does it say that in that -- you're talking about the chart?

MS. WEAVER: Yes.

THE COURT: Okay.

MS. WEAVER: And give me a second here because what we have on the demonstrative --

(Pause.)

MS. WEAVER: Actually, it's paragraph 146. So the ICO found that GSR obtained the following information from users who downloaded the My Digital app. And the very last phrase there is Facebook messages.

THE COURT: Okay.

MS. WEAVER: And then it reports the GSR obtained the following from downloading users' friends, and there's the list.

That does not include messages, but it includes photographs in which friends were tagged. We hadn't gotten to this point yet, but photographs contain geo-location data, time, all sorts of things. And if I shared in a Messenger with Derek a photo of us doing something I didn't want the world the see, and then he downloaded the app, the photo came through the app to GSR. And I didn't authorize that. I didn't know it was happening. So that's one kind of piece of information.

MR. LOESER: That's a hypothetical, Your Honor.

MS. WEAVER: So even if the settings were "public" during that four-year period, those photos that I didn't consent to, with all of that potentially compromising information -- in fiction -- would be available. So that's an example of a harm.

THE COURT: So remind me now, I've forgotten where the 1,500 users figure comes from? That's from their discovery responses?

MS. WEAVER: That is from their --

THE COURT: That's somewhere in the complaint?

MS. WEAVER: That is in the complaint.

THE COURT: Show me where that is in the complaint.

MR. SNYDER: Paragraph 139, Your Honor.

THE COURT: And thank you. Anybody should feel -- when I ask where is something in the complaint? If somebody knows, somebody from the audience, shout it out.

MS. WEAVER: That's why Josh is here.

So it says there about 1,500 people. It's the last sentence. And people who sent or received messages with those people potentially had their private messages accessed, as well.

THE COURT: So why shouldn't the analysis be for purposes of this complaint that's been drafted, given the sort of nonspecific allegation in paragraph 146 -- nonspecific in terms of numbers -- and the specific allegation here that about 1,500 people also gave the app access to their private messages, and people who sent or received messages with those people potentially had their private messages accessed as well; why shouldn't I say, Well, in light of these numbers there's not reason to believe that of the, you know, 80 million users -- was it 80 million?

MS. WEAVER: 87. They say 50 to 87. It's complicated.

THE COURT: Let's call it 80 million for now. Of the 80 million users who had their information stolen, quote-unquote, there are 15,000 users whose communications with their friends got taken. It's more than 15,000. It's about the users' communications with their friends, but it's a lot less than 80 million and why should we assume that the plaintiffs are among that group?

MS. WEAVER: Right. So very narrowly just about Cambridge Analytica, we don't know and we can't know until we get discovery. All we can say is right now we have standing for at least somebody whose messages were accessed.

THE COURT: Do the plaintiffs allege -- I can't remember -- do the plaintiffs allege that they used -- what's it called? Facebook Messenger?

MS. WEAVER: Yes. That is specifically in paragraphs 22-88. Every single plaintiff used Messenger and did it with the assumption that that would be private.

Just to circle back -- I know you wanted to only talk about the complaint. But if we were to amend, a significant number of them -- and it will be growing, I assume -- will confirm that they also in these kinds of messages used -- revealed privately information that is consistently used in what we call challenge questions. So hometown, place of birth, mother's maiden. The kinds of things that could also impair an identity fraud question, which we can talk about later, but I

just want to throw that out now.

MR. SNYDER: Your Honor, not to intrude on the seclusion of my colleagues, but --

MR. LOESER: You don't have a podium.

MR. SNYDER: I think it might be helpful to the Court, intruding as I am, to respond in realtime to some of these questions because there's both allegations in the complaint and other --

THE COURT: Well, just keep track of them and I'll -- you will get an opportunity.

MS. WEAVER: So question of --

MR. LOESER: You can tell one of us to sit down at any time, just to be clear.

THE COURT: I don't care.

MR. LOESER: The interesting thing about the question is we are at the motion to dismiss and we are drawing inferences in favor of the plaintiffs. And I think that's important and I think that that should be helpful in deciding whether these allegations are sufficient.

As to whether each of the plaintiffs had their messages disclosed contrary to their wishes, that's very easy for Facebook to determine that. They track this data. And they can tell us if that's true for these people.

THE COURT: Well, but that's not how litigation is supposed to work. It may be that, you know, maybe a government

agency should force them to determine that and disclose the information.

MR. LOESER: But isn't that kind of the nub of the issue that people actually have no idea what Facebook has done with their data? People assume that when they are instant messaging their Facebook friends it is not being made public. And now we're at a place in this case where we would like you to draw inferences in the plaintiffs' favor based upon their allegations that their messages were shared. And yet the answer we're getting back is it's not specific enough as to them.

It is a knowable question. It is very simple. Facebook could amend their interrogatory response and just tell us. It would be very easy. And it would also be something that they keep telling the world they want to be, which is transparent. Like, why should it be a secret whether these people know whether their instant messages are shared or not.

MS. WEAVER: And to add onto that. One, each of the plaintiffs received a message from Facebook saying: Your information may have been breached by Cambridge Analytica. So they know something.

Two, --

THE COURT: We know they're one of the 80 million.

MS. WEAVER: Yes. And, two, we know that they have reported all of this information to public agencies. But they

have -- I mean, the ICO has this. PricewaterhouseCoopers presumably has this. We have sought this. Even just the very narrow discovery about Cambridge Analytica, which we think is a sliver of the case, has not been produced here.

So even though -- you know, yeah, we're entitled to that. Not to state the claim.

But let me make two other points. There were tens of thousands of apps that this affected. So the odds that our plaintiffs had messages intercepted through some other app that was not Cambridge Analytica, that's an inference that should be drawn in our favor. Even --

THE COURT: I get that point. And I sort of came into this agreeing with that point as applied to everything except for Facebook Messenger. But I'm kind of understanding a little bit better your point as to Facebook Messenger. Okay. I get that.

MS. WEAVER: And then you must also get this. If Facebook says every now and then "We're only talking about one app," but we're not. They investigated 400 of them. We don't have the names. So if they gave us the names maybe we could go to our plaintiffs and find out. If you wanted to keep just for the apps.

THE COURT: That's never a terribly helpful response in a hearing on a motion to dismiss. Right? Because you're supposed to be able to have the facts that you need to state a

claim and stay in court before you do discovery, generally. And in this case it happens that you've done some discovery. Limited, but some.

MR. LOESER: And the reason why you allowed some discovery was so when the defendants denied something happened, it wasn't just creating a factual issue that could be answered by discovery.

THE COURT: Okay.

MS. WEAVER: May I move past apps? If you want to get to the threshold question of are we alleging Article III injury, the case isn't just about apps anymore. It's about business partners. And the bottom line is there was no disclosure that went to anybody about business partners. And as far as we know, business partners got everything that was in Graph API, Version 1.0.

THE COURT: And where are your --

MS. WEAVER: I'll tell you --

THE COURT: This is again potentially -- it's potentially the same inquiry whether you're talking about standing or whether -- or stating a claim. And I want to talk about business partners.

But before we go down that road -- it may be a long discussion -- I think it may be better at this point for me to give Mr. Snyder a chance to -- because I have the business partners on my agenda of things to talk about.

Before we lose the points that you wanted to make, why don't you make them.

MS. WEAVER: Wait. I have one other point, too. Which is the allegations at paragraphs 175 to 179 very narrowly talk about whether privacy metadata was retained on photos that came through Facebook Messenger.

THE COURT: Okay.

MS. WEAVER: And we understand upon information and belief that the privacy metadata that went with photos was stripped when it came through Graph API, Version 1.0, to app developers. And the way that that was discovered is that if you have a photo on your Facebook page -- I can't, but apparently people who know how -- could click on it and there is a piece of metadata that would reflect that your privacy setting was "public" there.

And app developers who then accessed photos that came through Graph API got the same photo. And when they looked, the privacy metadata was stripped off. And that makes actual sense; because if Facebook was going to give access to app developers, with regard to photos they were only supposed to do it within connection to -- they make this promise in their SRR's: We will only share data that is between -- and we will only use it with relation to the friend with whom you shared it.

If they were having app developers download all these

photos, they couldn't be like, I can only use this photo between Leslie and Derek. Or, the information. Or, I could only use this information between these people who sent the photos.

We allege that they stripped the metadata to make everything available to the app developers. And that is a violation of the privacy settings, which Facebook knows is a big deal. That's why they all the time are saying -- they're admitting that "We admitted by the privacy settings."

So the question wouldn't be just for the plaintiffs that we're talking about right now, are 34 of them, did they use Facebook -- were their Facebook Messenger messages taken. The question would be were their photos shared and taken. And your inference can be if they sent one photo to a friend -- actually, we should ask them if they sent photos to each other. Or, Messenger. That would have the privacy settings stripped. And I would argue that there's your Article III standing.

THE COURT: Okay.

MR. SNYDER: Thank you, Judge. So I'm going to address in the same order that counsel argued the four points. One was the consent and harm analysis, how they interrelate. Two is the "public"/"private" setting and how that relates, which is responsive to your question 1. And then three is the Facebook Messenger. And then I can answer any other questions or address anything else if you want me to continue.

THE COURT: Okay.

MR. SNYDER: So on the harm and consent. Yes, Your Honor, the consent analysis is dispositive here of the standing analysis. Because as I said, there's no plausible allegation of concrete harm where the plaintiffs have acknowledged -- as counsel just did -- that with respect to the API that all of the information was shared consistent with user consent.

And we've discussed at length that where privacy is concerned, any actual harm must be determined by looking at whether there's a privacy interest or a privacy right; which is always dependent on a reasonable expectation of privacy.

And here, counsel just acknowledged that all of the sharing on so-called API-1, which is the only platform at issue here with respect to third-party apps, was done consistent with user consent, user permission. Stated another way, the users understood that that information would not be private, but rather would be shared with friends, and then potentially with third-party apps.

And so again we look to the complaint's binding admissions 121 and 122, and again counsel's admissions here today, that there was consent. And as Your Honor indicated in the trespass context, if you invite me onto your property and I then enter your property, there's no harm unless I do something else. And what happened here was fully consistent with user consent.

So there's no injury, concrete or otherwise, if there's no

privacy interest due to consent. There's also no causal connection to the alleged wrongdoing, which is another fundamental standing element. Of course, you have to establish both a concrete and particularized -- not conjecture or hypothetical -- injury. But also has to be causally connected to the defendant's alleged wrongdoing. And here that fails as well since you can't have a causal connection to wrongdoing if the so-called wrongdoing was consented to.

And if you take the plaintiffs' argument to its logical extreme, an allegation that data was shared by itself would be enough for standing. And otherwise -- and in that sense there would be standing in every case. Of course, you have to look to allegations of harm and see whether they're plausibly alleged. And so --

THE COURT: That's a fair point, I suppose. But they do allege that -- let me ask you the question this way.

MR. SNYDER: Sure.

THE COURT: There's lots of data. There's lots of -- there are lots of things that we say an Facebook and things that we post on Facebook for our friends that we might want to keep private. Do you agree with that?

MR. SNYDER: For sure. You can actually keep it private to yourself. You can set it on the "me" setting. And people do that.

THE COURT: But you can also set it on the -- it's

hard to imagine why you would have a Facebook account if you wanted to have everything on the "me" setting.

MR. SNYDER: People do that because -- what they do, for example, creatives -- they'll spend a year creating content and just share with it themselves. And then when they're ready to launch it to the world, they launch it to the world. But they have so many choices. And here's the thing, Your Honor --

THE COURT: But let me ask you a question to make sure if I understand how the settings work.

My understanding is that as it relates to the issue of allowing your friends to share information with third-party apps, right? You can adjust the settings so that a great deal of that information cannot be shared by your friends with third-party apps.

MR. SNYDER: Correct. Those are the app settings.

THE COURT: Political affiliation, your religious affiliation, et cetera. Right?

MR. SNYDER: Yes. Users can make granular choices about exactly what information they want to share, with whom, what information their friends can share. Even they can opt out of apps altogether. And people do that.

THE COURT: And that may be very helpful to you in the context of, you know, your 12(b)(6) motion. Maybe it's even helpful to you in the context of your 12(b)(1) motion. But I'm bringing it up to respond to a specific point that you just

made which is that it can't be that the mere dissemination of data automatically gives rise to standing. I agree with you on that. But that's not what they're alleging.

What they are alleging -- whether they've adequately alleged it is a separate question. But what they are alleging is that there are lots of particular types of data that have been disseminated to third-party apps, such as religious affiliation, political affiliation, likes and dislikes, et cetera.

MR. SNYDER: And my point --

THE COURT: So that -- the allegations about the dissemination of that kind of data do give rise to standing if all the other requirements for standing are met.

MR. SNYDER: They do not give rise to standing based on the binding allegations of the complaint --

THE COURT: No. I'm just saying in general, they have not come in here and alleged that data has been disseminated. They've alleged that particular types of Facebook data has been disseminated that, if it was disseminated without their consent, would be a real problem.

MR. SNYDER: But they plead themselves out of court by acknowledging, as counsel admitted on the record here today, that any information that was disseminated -- any Facebook information that went to Kogan and then went to Cambridge Analytica -- was done consistent with the privacy choices made

by the users and the named plaintiffs themselves. So they've pled themselves out of court on injury because those choices they made to freely, willingly, voluntarily share their information with third parties negates, as a matter of law, any privacy interest they had in that.

THE COURT: Well, their response to that -- and we'll get to this in a little bit. Not that long now. We'll get to it in a little bit. But their response to that, of course, is that they didn't know that was their settings. They didn't know their settings allowed for that and Facebook misled them about that.

MR. SNYDER: Frankly, Your Honor, not to be flippant about it, the reason there isn't a case on point -- no disrespect intended -- is the plaintiffs, with no disrespect, you know, were chasing headlines here in this lawsuit before there was a cognizable injury.

THE COURT: It sounds like disrespect is intended.

MR. SNYDER: No. But, Your Honor, they've been searching or an injury from day one. We've been in this court, whether it's on the phone, and each time we've raised this Article III issue and it's been whack-a-mole because they keep on changing their theories. And now they want to amend again. Amendment is futile. The reason amendment is futile is because this consent --

THE COURT: Let's talk about that later.

MR. SNYDER: Okay. Let me get to the next point.

THE COURT: "Public" and "private."

MR. SNYDER: "Public" and "private." Of course it matters that they've failed to allege that their settings were "private" for the reason -- not "private" --

THE COURT: "Friends only."

MR. SNYDER: "Friends only" for the reason you said. There can be no concrete privacy injury when a user shares the information with the world; as a matter of logic, as a matter of law. And what's ironic is that the tort of the public disclosure of private facts, you know, requires publicity of a private fact.

THE COURT: Let me ask you a question about the public/private. You said there can be no concrete injury if Facebook shares information with somebody that has -- that has their setting at "public." Is that what you're saying?

MR. SNYDER: Concrete injury -- yeah. On the allegation of this complaint. Of course, if a thief took it and committed some impersonation crime or something else, there could be standing.

THE COURT: But just the mere disclosure of the data -- forgetting about what people do with the data -- but the disclosure of the data could never give rise to any sort of privacy claim if it's set to "public."

MR. SNYDER: On the allegations of this complaint,

correct. I mean, we can engage in hypotheticals about how a photograph of me on a "public" setting could result in wrongdoing by some malevolent actor. But on the allegations of this complaint, it's hard to imagine how there is a concrete privacy injury if the plaintiff has manifested no privacy interest in their information such that they are prepared for seven and-a-half billion people to look at it.

THE COURT: So I thought that Facebook had taken the position in litigation over whether it has to comply with subpoenas that even if a user's settings are "public," even if a user's settings are "public" --

MR. LIPSHUTZ: We're listening, Your Honor.

THE COURT: Do you want Mr. Lipshutz to answer?

MR. SNYDER: He whispered, "This is an argument I made in front of the California Supreme Court."

THE COURT: Yeah, I was wondering if Mr. Lipshutz was going to stand up for this question.

But Facebook has taken the position in litigation that even if a user's settings are for "public," under the Stored Communications Act, which is designed to protect privacy, Facebook cannot be required to turn over information from a Facebook user account -- Facebook user's account in response to a subpoena.

So it seems to me that that argument that Facebook has made in these other cases stands for the proposition that the

user can be injured, would be injured, if Facebook turned over information in response to a subpoena on a user who set their account for "public."

MR. SNYDER: Mr. Lipshutz is going to tell you why I respectfully and vehemently disagrees.

MR. LIPSHUTZ: Thank you, Mr. Snyder.

The Stored Communication Act prohibits Facebook from disclosing information pursuant to a subpoena absent consent. There is no "public" and "private" distinction in the SCA when it comes to --

THE COURT: But your whole argument in this case is that there's no "public" and "private" distinction because -- or, one of your arguments in this case -- I shouldn't say your whole argument -- one of your arguments in this case is the one that Mr. Snyder was just making which is if the Facebook user sets their privacy settings to "public" as opposed to "friends only," then there cannot be any privacy expectation. There cannot be any privacy injury, there cannot be any privacy expectation.

If that's true, how could it be that the Stored Communications Act prohibits Facebook from turning over information on users in response to a subpoena when the user has set their privacy settings at "public"?

MR. LIPSHUTZ: Because the Stored Communication Act provides a series of procedures that have to be followed in

order for Facebook to turn over information. One of those procedures is obtaining the express consent of the user. Facebook conceded, as Your Honor will remember -- I believe Your Honor was there for the argument that day. Your Honor will remember that we conceded at that argument that a "public" setting --

THE COURT: I never would have gone if I'd known that I was going to get assigned this case.

MR. LIPSHUTZ: Of course, Your Honor. This was long before.

Facebook conceded at that argument that a "public" setting by a user can be used to imply consent for purposes of the SCA. And actually, that's what the California Supreme Court held. The California Supreme Court held that when a user sets their information to "public," they have no reasonable expectation of privacy and they've effectively consented for purposes of Stored Communications Act.

That is now the settled law in California. Facebook still does disagree to some extent with that decision because the touchstone of the analysis in the Stored Communications Act context is consent. It's not "public" versus "private."

What Mr. Snyder is talking about here is a reasonable expectation of privacy in the context of the common law. Because when you allege a procedural violation of a statute, like the Stored Communications Act, you must show that the

injury you're alleging has an analog in the common law in order to have standing under Article III. The only analog that that injury could have in the common law is public disclosure of private facts. That requires an expectation of privacy by the user. And there is no expectation of privacy where the user has set the setting to "public."

THE COURT: But maybe your argument in that context stands for the proposition that even if I -- if my settings are at "public," my privacy settings are at "public," which means any member of the public who's out on the internet can see my photographs or see my wall posts, that is still somehow different from Facebook giving -- sort of giving access to a company and allowing the company through Facebook's own system to collect all that data about the user.

MR. LIPSHUTZ: For purposes of whether it's a Stored Communications Act procedural violation, I think there may be a difference there, and that's the position that we've been taking. But for purposes of expectation of privacy from a common law privacy right perspective, I don't think there is.

MR. SNYDER: And Your Honor --

THE COURT: Well, but another way to put it -- this may be bleeding into the merits of the Stored Communications Act claim -- but another way to put it is if you set your privacy settings at "public," does that mean that -- does that in itself -- I understand you have this other language about

the app settings that talks fairly explicitly about what apps can get from your friends, right? But for now, just focusing on the fact that the plaintiffs have not alleged that their settings were not on "public," does than mean that they have consented to Facebook allowing third-party apps into the system to pull out all of this information about them?

MR. SNYDER: It means, Your Honor, that in looking for a common law analog, or a common law privacy interest, you have to find actual harm. And on the allegations of this complaint where they have consented and where if they're on "public" allow the world to get everything, there's no privacy injury.

But let me just pivot, Your Honor. Because even if they were "friends only" for the duration of the class period --

THE COURT: I want to hear this, but I have one other very quick question that I want to make sure I don't forget.

They said that during the class period -- during a good portion of the class period -- the default settings were not "public." The default settings were "friends only." Do you have an answer to that?

MR. SNYDER: I don't. But I do know it's not alleged in the complaint. And I do understand the default settings may have changed from time to time. But it doesn't matter to question 1.

THE COURT: Is there any -- I'm happy to hear why it doesn't matter, but is there anything I can look to in the

complaint or in the materials that you believe are judicially noticeable, that would allow me to answer that question?

MR. SNYDER: I mean, all we have is the language in the complaint, which we have to accept as true, which quotes user -- the user agreement term which says that if you have made that information "public," then the application can access it just like anyone else. And goes on to talk about how you can control the information by using your app setting.

So what they have in the complaint is no allegation of whether they were "public" or "private," no allegation of when the app sharing was set to "public" or "friends only."

But it doesn't matter, to answer your first question in the order number 16. Because even if they were set to "friends only" for the duration of the class period, every named plaintiff, it is still -- failed to standing because you can't have a concrete privacy injury when, again -- to beat the horse even more -- a user authorized the friends to share their information with third-party apps.

And so, in fact, again, we make the affirmative point. And reason why their privacy harm argument is a little bewildering is the sharing that they complain of in the complaint is consistent with the very decision the named plaintiffs made through their privacy settings.

And so the very purpose of Facebook is to share information with friends and others. They shared information

with friends, friends share that information with third parties consistent with their settings --

THE COURT: I get your argument.

MR. SNYDER: So it's a red herring whether it's "public" or "private" because the same result obtains. They've consented, which negates injury, which means under 12(b)(1) they have no standing.

THE COURT: The red herring I guess that you raised, because you raised in your papers that they didn't even allege that they didn't have --

MR. SNYDER: No. It's more absurd if it was "public," but it's equally non-actionable as "private."

Let me get to the Messenger.

THE COURT: The Messenger. Yes, please. And then after that I'll turn back to them. Because I actually think that your points that Facebook disclosed in relatively clear language that, you know, third-party apps were going to have access to a user's information through a user's friends is a pretty strong one. And it's going to be mostly them I need to hear from on that.

MR. SNYDER: But they went even further than that, to their credit. They said not only will your information be shared or re-shared, but once -- and this is just logic from time immortal -- when you send a letter to someone it's a spent arrow. You never know what they're going to do with it. And

everyone knows --

THE COURT: I don't agree with that. I don't think that analogy holds. I mean, when you send a letter to somebody, you -- I think what you are trying to do, and one of the real problems I have with Facebook's argument, and it's something that I think is probably inconsistent with what Facebook really thinks, is that it's binary. Either you have an expectation of privacy or you don't. And you seem to be saying with your analogy to sending a letter --

MR. SNYDER: No, Your Honor. Because I could qualify every single one of my answers with: So long as Facebook is respecting the user's choice. Because Facebook scrupulously honors the user's choice.

THE COURT: No. But you're -- but this analogy to sending a letter, "Hey, when you send a letter to somebody you never know what's going to happen to it," no. I mean, sending a letter to somebody is different from shouting something from the rooftops. You have -- there is -- maybe you don't have as strong an expectation of privacy in that information as you did before you sent the letter, but you still have an expectation of privacy after sending the letter that is greater than if you shout it from the rooftop.

MR. SNYDER: My point was narrower than the one you've described. My point is that Facebook made clear to users that if they consent to sharing their information with friends, and

consent to their friends sharing their information with third parties, Facebook can't control -- although they'll do their best through their agreements with their partners -- Facebook can't control what that third-party might do with it.

And so -- and they specifically warn users of that and then say: You have choices to make. You can protect yourself. If you don't trust an app that might have your information, you can protect yourself in a myriad of ways, including by opting out of apps entirely, by not sharing information with apps, and ultimately you can go off the platform entirely if you don't trust it.

And so users have myriad options which differentiates this case from every single Article III case where standing is found where there is an actual concrete harm by an intruder who is up to no good trying to harm that third-party.

THE COURT: And all of that hinges on whether Facebook adequately disclosed that this was going to happen.

MR. SNYDER: Yes.

THE COURT: Like I said, I'll talk to them about that. But you wanted to talk about --

MR. SNYDER: Messages. Again, there is a lot of conflation and inflation of points here.

The point on messages is if you go to both the argument counsel made and paragraph 115 of the complaint, it's clear that Kogan used API-1 only in connection with the This Is Your

Digital Life app. It's clear from the complaint and from counsel's statements that all information shared, including messages by users, was shared consistent with their privacy settings.

What happened was for a period of three months or so Kogan's app was obtaining messages. From users only, by the way. Not from friends. And 1,500, not --

THE COURT: But it's messages between users and their friends, right?

MR. SNYDER: Right. But as the chart on 145 shows in the complaint, it was only users who downloaded the app whose messages, message file folder, was shared for a brief period of time with Kogan. It didn't give access to a user's friends messages at large. It was just what was on their message.

THE COURT: And that is -- to make sure I understand that. That is in contrast to the other types of information?

MR. SNYDER: Yes.

THE COURT: In other words, for the other types of information, like somebody's wall posts and whatnot, it doesn't merely give access -- the friend didn't merely give the third-party app access to communications between the friend and the user who's complaining about their stuff being taken than any other communications that user engaged in with other friends, wall posts, what have you.

MR. SNYDER: Correct. And that's depicted in the

chart that the plaintiffs have on 145. So the messages that were shared through API-1, which they admit was the only -- was the only application at issue here, they were shared consistent with the privacy settings. That is, they were shareable. So it stands in the same category as all of the other information shared by the named plaintiffs.

That is, it was shared with their consent. It was shared freely, voluntarily, knowingly. And for the users, it was shared so that they can get a dollar each. I mean, we know that, right? So even in this case, it was -- the user downloaded the app, they got paid a dollar, and they knew what they were giving in exchange. They were giving what was depicted on the chart on paragraph 145.

So there is no harm as a matter of law to a user who takes a quiz, gets paid a dollar, and voluntarily in exchange, with consent and with full warning and notice, gives up their personal information, including their messages.

Now, that is separate and apart from the wildly speculative nature of the harm allegation with respect to messages. Because, again, only 1,500 out of 300,000. Only a small fraction of Facebook users overall had messages obtained by Kogan during this three-month stump period. And so that's a separate reason. But you don't even need to get to the speculative, so hypothetical nature of the claimed injury, because again Kogan obtained Facebook messages only from users

who downloaded the app and gave their consent.

So I think that no -- again, not to jump the gun, but there's no amendment here that can cure that, really.

THE COURT: We'll talk a little bit --

MR. SNYDER: Do you want me to address affirmatively the consent point or do you want to hear from them?

THE COURT: I want to hear primarily from the plaintiffs on that.

MR. LOESER: Your Honor, before I lose the chance to say it, with questions that need to be answered, I do want to make sure that we are literally answering the exact questions that came to us last night because I think that those really hit the nail on the head on some key issues.

And the first question you ask if people -- if it's not clear whether people changed their settings from one setting to another, is there no claim. And I think it's important also to consider --

THE COURT: I thought the question I asked is does that matter from a standing --

MR. LOESER: Correct. And I think another point worth making on that is that that question assumes that if the disclosures had been meaningful -- and we say they're not --

THE COURT: Yes, yes.

MR. LOESER: -- that people wouldn't have done something different. That's another one of those inferences

that I think is fair to draw in the plaintiffs' favor. So I think that's an important point.

I also just want to direct the Court in our presentation on page 7 there are some statements that have been made by Facebook executives that really stand in such stark contrast to the way counsel is describing. Counsel has described for you a world in which Facebook scrupulously complied with all of the users' settings and made it abundantly clear -- it's so clear, Your Honor, it can be decided as a matter of law at this stage.

Well, but contrary to that, you have the statement -- and these are mostly from Mr. Zuckerberg. Breach of trust between Kogan, Cambridge Analytica, and Facebook, but it was also a breach of trust between Facebook and the people who share their data with us --

THE COURT: Can I just ask you -- so these -- these statements are relevant to what? To what claims that you make?

MR. LOESER: These statements, for one, they're certainly relevant to all of the privacy-related claims. They're directly relevant to --

THE COURT: They're relevant to the privacy-related claims, I guess you're saying, because these people who made these statements are admitting that they misled users about what was happening with their data?

MR. LOESER: They're admitting facts that undermine the basic tenet of most of your questions; which is, was the

disclosure sufficient? They're admitting facts also that undermine the notion that all users' settings were complied with.

THE COURT: But saying we need to fix that is --

MR. LOESER: Well, what's the breach of trust, Your Honor? What's the breach of trust if they did everything they told people they were going to do?

If you go to the next one, they say: We have a basic responsibility to protect people's data. If we can't do that, then we don't deserve to have the opportunity to serve people. We've heard loud and clear that privacy setting and other important tools are too hard to find and that we must do more to keep people informed.

These statements are directly contrary to what you've heard. And the reason why it matters here and now is we are at a motion to dismiss, and we are drawing inferences in plaintiffs' favor. And they're coming in and arguing very factually -- like "scrupulously" was the word counsel used. We scrupulously complied with everything users wanted.

Well, that's inconsistent with testimony. And some of these are statements to the media, others are testimony under oath to Congress. So I just think that's a point worth making.

THE COURT: I don't know if there's as strong of an inconsistency between these statements that you're showing me and counsel's statement that we scrupulously complied with

people's privacy settings, right? I think the point is that -- the point that you want to make is that even if Facebook scrupulously complied with people's privacy settings, people didn't know that that's what their privacy settings were. Right? Or, people weren't given sufficient notice that unless they changed it, their default privacy settings would allow for third-party apps to get basically all of their Facebook information.

MR. LOESER: Those are two entirely fair inferences to draw from these statements. So is the inference that they didn't do what they are said they were going to do. But I get your point --

THE COURT: No, that's the point you're making. You're not arguing that Facebook violated its own privacy policies, it seems to me.

MR. LOESER: Correct.

THE COURT: It seems to me that what you're -- okay. Let's take a step back. I get these statements and I understand your theory of relevance of these statements.

Let me tell you the problem that I think I have with your allegations about the issue of consent, okay?

It seems to me from your briefs from your complaint that you are primarily arguing that Facebook misled users and concealed from users the fact that unless you change your settings third-party apps are going to be able to get all of

your Facebook information from your friends.

And it seems like from the disclosures -- from the disclosures that Facebook made -- that it didn't exactly conceal that. It didn't exactly mislead users on that point. It might be -- maybe I'm wrong about that. And I'll give you a chance to go through all of the language with me.

But it seems to me that even though that seems to be the thrust of your complaint, the real complaint here, it's not that Facebook said anything misleading, but that given the importance of the privacy interests involved, given the significance of the fact that third-party apps could go in and interact with your friends in a way that allowed them to get all of your information, given how big of a deal that is, the disclosure should have been much more prominent and much more clear and Facebook should have brought this to the attention of their users in a much more sort of -- in a louder, more jarring way and given them more clear instructions for how to fix it.

So, for example, something like, when you're signing up, you know, for Facebook, you know: Under current settings third parties will be able to obtain all of your information, or virtually all of your information, simply by asking your friends for it. If that's important to you, here's what you need to do to change your settings to prevent that from happening. Or to prevent that largely from happening, other than like your name and your gender and your hometown and

whatnot. And that Facebook, they didn't conceal, they didn't mislead, but they didn't do a good enough job of bringing this to the attention of the users given the importance of the privacy interests at stake.

And then to circle back to the statements from the Facebook executives that you were just pointing me to, I think that probably is one way to interpret what they were saying when they say, you know: This was a breach of trust, and we messed up, and we have to do a better job of protecting your privacy.

So one question I have, before you disagree with me and explain to me how, in fact, Facebook did affirmatively mislead people, I want to ask you: Why didn't you tee up your complaint in that way? Is it that the law allows Facebook to do that? That there's nothing in the law that as long as Facebook is sort of accurate about what it describes there's nothing in privacy law that requires Facebook to do it in a clearer or more prominent way when the privacy interest at stake is so significant?

MR. LOESER: Your Honor, I think what you've described is, in fact, what we've alleged. So we have alleged that they were affirmatively misleading, as you state. But we've also alleged in spades that the way they presented this information resulted in people not being informed and being misled.

I also think it's important --

THE COURT: Right. You have alleged in spades that people have been misled. But what I'm asking is -- in other words, let's assume that Facebook didn't actually do anything -- didn't actually say anything inaccurately. Let's say Facebook got together with its lawyers and its other sophisticated messaging people and was very careful to make sure that it did, in fact, accurately disclose what would be happening; it just didn't do it in a prominent enough way given how important the privacy interests are. Does the law say that that in itself could be a privacy violation?

MR. LOESER: Yes. Because they've omitted so much essential information. What you described was a textbook example --

THE COURT: I guess I would disagree with you. I don't think they've -- we'll get to that.

MR. LOESER: They provided an explanation --

THE COURT: What I'm asking is you keep saying "misled" and "omitted." But I'm saying if they didn't say anything that was misleading in their disclosures and they didn't actually omit anything, but they merely did not do a good enough job of bringing it to users attention and did not do a good enough -- provide prominent and clear enough instructions for how to fix the problem, if you think it is a problem that third-party apps can get all of your Facebook information; could that itself give rise to a privacy claim?

I don't think I see that in your complaint or in your papers anywhere and I was curious why you didn't tee it up to that way. And I was thinking, well, maybe they didn't tee it up that way because the law allows Facebook to do that. Like the law doesn't --

MR. LOESER: I don't think the law allows them to do that. And I also think there's an important merging of doctrines in what you're describing. One is the doctrine of disclosure and the other is the doctrine of consent.

And the problem and the way -- the reason why we've described both in our briefs and in the complaint what happened here is we have two problems. We have what you're describing as the affirmative misrepresentations. I'm saying that in the world of fraud and negligence and other things there's a distinction between omissions and affirmative -- and we have both omissions, things they didn't say that would have made statements clear, and we have affirmative misrepresentations.

But when you venture into the conversation we're having now, you're getting into the world of consent. Facebook's entire argument about why none of these claims are legitimate is they claim that the users, the plaintiffs, all consented. And consent is an issue of contract.

And so when you're trying to sort out whether there is consent, you have to figure out whether, in fact, people have been informed sufficiently so that they enter into that

contract it's lawful and binding. And that is what's lacking. And it's what's lacking in your description of what happened here. What's lacking is actual lawful consent.

THE COURT: Well, could I ask you about that? Because it seems to me that there are different kinds of consent. There's express consent and there's implied consent. And as I understand it -- I mean, Facebook probably -- and I don't think either of you really teased this out in your briefs and I'm not sure it's quite teased out in the complaint. Although I'm not sure it has to be teased out in the complaint.

But I guess what I understand express consent to be is, you know, "I hereby acknowledge that I am --" you know, "I understand that this is what's going to happen and I agree to it." And you sign something or otherwise manifest your assent it to. And then there's implied consent which I sort of think of more as a disclosure issue. I think to say implied consent, you know, the word "consent" is almost misleading. The point is that whether you affirmatively, explicitly consented to it, Facebook adequately disclosed to you that if you use its service this is what's going to happen to your stuff, right? And so --

MR. LOESER: Which is an inherently factual determination to try and sort out.

THE COURT: That it adequately disclosed to you --

MR. LOESER: Yes.

THE COURT: Why?

MR. LOESER: Well, when we get there -- and we will get there -- we're saying that these disclosures were misleading, they were incomplete --

THE COURT: But you said it's an inherently factual --

MR. LOESER: In this case it is inherently factual.

THE COURT: In this case. All right.

MR. LOESER: I'm sure you can find one, and counsel has pointed to some, like the *Smith v. Facebook*, where there was a disclosure, "We tracked your browsing on when you visit websites," and the plaintiffs sued them for tracking their browsing when they visited websites. That's the kind of thing where you could look at that and say it's not factual.

THE COURT: But there are different kinds of consent, right? I mean I guess --

MR. LOESER: There's a lot of law on that.

THE COURT: Yeah.

MR. LOESER: There's a lot of law on different kinds of consent. And you know where it comes up? Is in click-wrap and browser-wrap agreements. And that's the world that Facebook lives in. They have these documents they present online, and they are supposedly obtaining consent.

And this is a really important point about disclosure. All of these disclosures that counsel keeps talking about and their brief discusses are things that they are saying that they

claim as a result of which there was binding lawful consent. They aren't saying there was implied consent, and that's something else altogether. They're saying that there was actual consent.

And they don't cite the leading Ninth Circuit case on this, which is the *Nguyen v. Barnes and Noble* case, which is a bit bizarre because it is controlling. And that case addresses specifically when a document that you present to someone online -- and it's 763 F.3d 1171, Your Honor, 2014.

The specific issue in that case -- the issue that keeps coming up in the technology online world, which is that when you throw up your terms and use and data policies and other things, are they lawful, bindings documents? And often it comes up in the arbitration clause context because one of these documents may have an arbitration clause in it. And so the companies are often saying, Well, you agreed to it. You impliedly consented because you used our website.

And the Ninth Circuit has looked at this a couple of times, and made very clear in the *Nguyen* case, what it really means to obtain lawful consent to make something part of a contract.

And they look specifically at the different kinds of things that companies do. And they identify click-wrap. Click-wrap is when you have to go on and affirmatively acknowledge that you accept the terms. Okay? Browse-wrap is

this other thing where instead of doing that you have a disclosure that says, If you continue to use our website you agree. Or sometimes there's an acknowledgment where you click on the document and there's another indication of assent.

And here -- and this again gets into this sort of deeply factual nature of this whole discussion.

If you look at what Facebook has done with the data policy -- and the data policy is where all of these disclosures come from -- they started out -- and I'll bore Your Honor with the details because it's a very factually specific argument. But they started out, and from 2009 through 2012 they had a type of browse-wrap, and that's page 24 of the outline.

THE COURT: Page 24 of the outline. Is this -- is that all --

MR. LOESER: The presentation. I'm sorry.

THE COURT: Is that all embedded in the complaint?

MR. SAMRA: 261, Your Honor.

THE COURT: Paragraph 261.

MR. LOESER: The reference is on -- Yeah. So they start out --

THE COURT: Is this a page of your outline?

MR. LOESER: On page 24. And this is the sign-up that they were using in the 2009 to 2012 point. And, again, if you go to *Nguyen* and Ninth Circuit case that controls whether these things create actual contracts, the court talked about how

conspicuous the browse-wrap indication needs to be and whether there's affirmative assent.

And so from 2009 to '12 you have this first page where you actually sign up. So you sign up and agree before you get to the second page. And on the second page, which is page 25, you have this whole collection of confusing information. And again when you read *Nguyen* and the other cases that talk about browse-wrap issues, they talk about placement of this information and whether it's conspicuous or not. But at least in 2009 and '12, as inconspicuous as it was, you said by signing up you're indicating you have read and agree to the terms and use and privacy policy.

So we don't think the privacy policy says what it needs to say to be clear, but at least in this time period you would do something along the lines of what the *Nguyen* court, at least with regard to that acknowledgment, some type of indication of assent. Now, it may well not be binding and appropriate because it's confusing and hard to find, but at least they use the word "agree." Facebook does this all the time with the disclosures and the policies that they're relying on, they're constantly changing.

So when you get to the 2012 to 2018 time period, it's really kind of strange. And perhaps too cute by half. I don't know why they suddenly wanted to take away the word "agree," but in that time period when you clicked and signed up all you

clicked was something that said "you agree to our terms" -- that's the statement of rights, responsibilities of the terms of use -- and that you have read and understand our data policy.

So that is not -- under *Nguyen*, there's no assent. There's no agreement. The agreement -- who knows. Like it will be a really interesting question in discovery, why did you take out the actual agreement to the data policy? And the reason why I'm kind of harping on this now was that all of the disclosures --

THE COURT: I instruct you to refuse to answer that question on privilege grounds, because I think probably how that's going to go.

MR. LOESER: Exactly. Unless they want to make some type of advice of counsel claim in here. But they took it out. They took out the agreement. And it's really significant because this basis on which you're evaluating whether to dismiss this case of disclosure ties into whether there was a contract. Whether there was --

THE COURT: Well, that's the question I have. I mean, that's one of the questions that's been bothering me about this case. Is I understand -- you know, I understand that sometimes they asked for you to agree to the -- and sometimes they didn't.

Go ahead.

MR. LOESER: Before I lose the thread, just let me emphasize again. For the language that they're pointing you to to be effective and to provide a basis for which to conclude as a matter of law that there is consent, there has to be a contract. And under *Nguyen*, specifically for the 2012 to 2018 time period, there cannot be a contract under controlling Ninth Circuit law. They took out the word "agreement." Who knows why.

Now, Your Honor, if you look at the next page -- this is page 27 -- after Facebook becomes a front page news story over and over again, after Cambridge Analytica, after all these other disclosures about all the other things that they're doing that people didn't realize, they changed this sign-up form again. And look what they've put in this time: By clicking 'sign-up' you agree to our terms, data policies, and cookie policies.

So they've put the agreement back in. So the problem with their argument is they're trying to get you to decide as a matter of law that there was lawful, binding consent. But for much of the class period they didn't have it. And they messed around with it and they put it in and they took it out.

THE COURT: But one of the things that I'm having my -- having a hard time wrapping my head around is -- I quoted you here, I think. I wrote it down as you were saying it: For consent there has to be a contract.

And if you define implied consent in the way that I've defined it, does there really have to be a contract? In other words, as I've been reading your complaint and your papers I've been scratching my head wondering: Why are they making such an effort to establish that there was not a contract as it applies to the --

MR. LOESER: Well, let me make it crystal, crystal clear. There's a contract based upon the rights and responsibilities.

THE COURT: Right. Everybody agrees. Everybody agrees on that.

MR. LOESER: There's nothing in the terms of use.

THE COURT: But why does that matter, is what I'm asking.

MR. LOESER: It matters because all of the language that they said provides this concept of legally binding consent, such that you can decide at this stage of the case that these disclosures mean you have to dismiss the case; all those things are not in the statements of rights and responsibilities. They're in the data policy.

THE COURT: Okay. So let me ask you this question. Let's say that Facebook did what I think it should have done. Which is -- not as a legal matter, but as a matter of providing good service to its users. Let's say that Facebook didn't say anything about sharing with third-party apps in the contract

that it entered into with users. But, it disclosed very prominently to users: Alert. If you don't change your settings, millions of companies will been able to access all of your Facebook information. Or, virtually all of your Facebook information. So if you don't want millions of companies to access virtually all of your Facebook information, please follow these four steps for changing your settings.

And, you know, you link to the steps and you make it really easy for even somebody like me to understand. Right?

That, then, would not be part of the contract. But I would think that it would be adequate to protect Facebook against a claim of privacy violation. And if I'm right about that, then my question is: Why are you placing so much importance on the fact that this disclosure was not in the contract?

MR. LOESER: I think the answer comes back to this *Nguyen* case and all of the case law that deals with the issues of effectively what is consent. Whether you accepted a document as part of a binding contract. And I think the way Facebook has presented its motion --

THE COURT: But I think that maybe is not responding to what I'm saying. Because I'm asking: Why does it have to be part of a binding contract to protect against a privacy claim? If the company does a good enough job of disclosing the ways in which your privacy interests will be interfered with,

and does a good enough job of explaining to you how you can protect against that, why does it matter whether it's in the contract?

MR. LOESER: I think it matters because the doctrine they're relying on to dismiss this case is the doctrine of consent, and that is a doctrine that is contractual in nature. All of the cases that we cite, and that they cite, that have addressed this issue address the question of whether they have obtained lawful consent from you, based on those disclosures.

And again, if you look back at these browse-wrap cases, they're effectively saying -- the defendants are saying: We have implied consent. You continue to use our services. Therefore, we told you, you use our services, you know, these are the terms.

And the courts look at that and say: Wait a second. We're into the doctrine of consent, which is a concept of contract law. And the way you obtain consent is through having an actual agreement. And you get that with an indication of assent.

I think that's the best answer I can give you on why -- where we are now, based on their motion, why we've put so much emphasis on whether these data policy statements are in a contract. Because they're trying to use the data policy to establish something called lawful binding consent. And they can only do that if there's a contract.

And let me add one more --

THE COURT: But I don't know if that's -- I mean, again, you know, the courts have this thing that they call implied consent. And I think implied consent doesn't necessarily equal contract. Binding contract. Right? It's the kind of thing that you talk about, you know -- you know, if you -- let's get it out of the -- let's take it out of the internet and just say, you know, there's a sign-up. And you say -- and the sign says, you know: Warning. You know, there are some -- there's some potholes. Whatever. There are some hazards. If you enter this building there are some hazards that you should be aware of. And you enter the building and you are injured by one of the hazards you might say, well, there's no binding contract between you and the owner of the building, but there's kind of implied consent or assumption of the risk or -- I don't know what the term would be. But I think sometimes courts call that implied consent. Right? You consent to taking on that risk.

And so I would think that in my hypothetical, you would say, there was implied consent because Facebook did a good enough job of notifying the user of what was going to happen with their information. And the user continued to use the service without changing their settings.

MR. LOESER: Yeah, I --

THE COURT: But there's no contract.

MR. LOESER: I think the functional effect of implied consent is that you're saying there's an agreement.

THE COURT: Okay. Maybe I'm misunderstanding the concept.

MR. LOESER: Is a contract. And, again, that's kind of what the case law looking at browse-wraps deals with. Is that they're saying: We give you this information and you kept using. It's implied consent.

The court's saying if your argument is consent, if you're saying there was an express -- this is what Facebook has said. There's lawful express consent. Which, mind you, is something the FTC told them they were supposed to be getting from people, and then they didn't. I'm not sure what else we can do with the issue other than to tell you that I think it's hard to separate those things. It's an important issue.

THE COURT: That's helpful. Why don't I suggest --

MR. LOESER: Can I make --

THE COURT: We've been going for --

If you need to make a short point, go ahead.

MR. LOESER: Very short. Before we get into the details of these disclosures, I think that it's important to retreat back to motion to dismiss. We're talking about consent. There are reams of cases. And I do want to provide you and your clerks with the cases we think are the best ones -- we can do it after lunch -- which deal specifically

with why you don't determine consent, whether implied or express, at a motion to dismiss. And why it's just an inherently factual thing. And the reason why it's so factual is that for consent to be lawful -- and again, whether it's implied or express -- the disclosure has to line up exactly with the conduct. And that's what is -- they're miles from there.

THE COURT: Why don't we -- we've been going for two hours. More than two hours. Sorry about that. Why don't we break, have lunch. Not together, of course. And we'll come back at 1:30 and we'll continue this discussion. And we will start with you walking me through the language and explaining why the language was misleading or didn't adequately disclose what was happening with people's information.

MR. LOESER: And if I may, as well, just providing that list of cases which I think is --

THE COURT: Of course. Of course. But where is the -- so pick your best language. Right? There are different iterations of the language. Pick the version that you think is most misleading and walk me through that one.

MR. LOESER: We have some of that in the presentation and we can point some language out.

MR. SNYDER: Your Honor, if I may just ask. May we leave our stuff here?

THE COURT: Yes. Well, wait a minute. I should --

THE CLERK: Yes.

THE COURT: Is that okay?

THE CLERK: Yes. No problem.

MR. SNYDER: For those of us who are traveling, do you have an end time for today? We can stay until midnight if you want, but I just want to know.

THE COURT: I don't have a hard stop. I was assuming we might take another hour or two this afternoon.

MR. SNYDER: Great. Thank you.

MR. LOESER: We're fine proceeding without counsel, Your Honor.

(Recess taken at 12:38 p.m.)

(Proceedings resumed at 1:35 p.m.)

THE COURT: Could I please ask one more standing question?

MR. SNYDER: For me?

THE COURT: For you, I think.

MR. SNYDER: Should I stand?

THE COURT: Sure, come on up. I don't want us -- I'm going to try to prevent us from going down that standing rabbit hole again because I know there's still a lot of stuff that you both want to talk about.

But I think it's worth asking you this one other question.

MR. SNYDER: Yes, sir.

THE COURT: Can you give me an example -- like,

assuming your theory of standing, can you give me an example of a Stored Communications Act case where the defendant would prevail on the issue of consent on the merits, but not prevail on the issue of consent on standing? In other words, does your position stand for the proposition that every single Stored Communications Act case where the defendant wins on consent is a case where the defendant wins on standing.

MR. SNYDER: Well, let me start with the merits point which is that obviously there needs to be an unauthorized disclosure of electronic communications under the Stored Communications Act. So if there's authorization there is, by definition and text of the statute, --

THE COURT: -- no violation of the statute. But I'm asking you if you can give me an example of a case where a defendant would win on that defense on the merits, but not on standing. Or is every single Stored Communications Act case where consent was given a case that the defense wins on standing?

MR. SNYDER: You know, it's a hard question, Your Honor, and I'm not dodging it. Because the SCA reflects Congress's judgment that electronic communications that are stored by service providers should receive certain protections, right? That are similar to those that existed in the analog age.

And so most cases brought under the SCA arise not in the

context of this case where you have -- you know, so the answer is I don't know. I'd have to know all the facts. But I do think that in this case -- not dodging the question -- that the analysis does collapse because the consent is dispositive here of standing, whether it's contractual, implied, or otherwise it doesn't really matter.

THE COURT: And I think that's the -- that is potentially the problem with your argument. Is that if it collapses here, it collapses in every Stored Communications Act case.

MR. SNYDER: I don't think so.

THE COURT: So you're dismissing every one on the standing.

MR. SNYDER: I don't think so, Your Honor. I think you have to look at the -- we're not making a blanket statement about the SCA. And as all SCA cases that analyze standing, you have to analyze the particular allegations of each case. So I can't answer a hypothetical without knowing what the factual allegations are. What I can say in this case --

THE COURT: I know what you say in this case. You don't need to say it in this case again.

MR. SNYDER: So the answer is I don't know. It depends on what the facts are. I can imagine -- I mean, there are --

THE COURT: If you can imagine a scenario, tell me

about it.

MR. SNYDER: I don't know, Your Honor. I haven't thought about it, frankly. I can think about it and get back to you on it. But I don't think -- I don't think that we're saying that in every single SCA case if there is consent there's no injury. Because I would need to know what all of the hypotheticals are.

For example, maybe --

THE COURT: No. I'm saying if there's consent, there's no standing.

MR. SNYDER: Well, no. Maybe the service provider did something else that caused injury even with the consent to the user. And so there could be consent but some other articulated harm that occurred as a result of something the service provider did in routing and storing the information. And so I would need to know what the facts are to give you an answer.

THE COURT: You mean if the service provider did something else wrong with the information.

MR. SNYDER: I mean, if the service provider was, you know, in business with a thief and conspired with a thief and changed their app settings for the purpose of obtaining information so a thief could commit identity fraud.

THE COURT: Then the service provider might be liable for theft. But under your theory, I think there would be no standing to assert that they're liable under the Stored

Communications Act.

MR. SNYDER: Well, the Stored Communications Act requires a threshold, as an essential element, unauthorized access. Unauthorized disclosure. That's the gravamen of the offense.

THE COURT: I don't know if it's an actual element, no. It says you're not allowed to disclose this information unless --

MR. SNYDER: -- you have authorization.

THE COURT: -- and then there's a list of exceptions. And one of the exceptions is the person gave lawful consent.

MR. SNYDER: Correct. And in this case on these allegations there was --

THE COURT: I'm not asking you about these allegations. Not asking you about this case. I'm asking what your position stands for with respect to the Stored Communications Act. If you don't have an answer, that's fine. I myself can't think of an answer, either, and I've been thinking about it longer than you have.

MR. SNYDER: Sure.

THE COURT: Let me ask you one other -- I told you I was going to ask you one standing question. I want to ask you --

MR. SNYDER: Sure. I hope it's not as hard as the last one.

THE COURT: Maybe not. Okay. Let's say you have -- trying to think of other contexts in which this concept would present itself, right? And one good idea that my law clerk came up with was let's say you have a 1983 case where you're suing the government for violating the Fourth Amendment. Right? And you say, Well, I put my garbage out and law enforcement officers came and searched through my garbage, you know, in violation of my Fourth Amendment rights.

Now the answer to that is you lose on the merits because you have no reasonable expectation of privacy in the garbage that you put out. But would a court also dismiss that 1983 case for lack of standing because you have no reasonable expectation of privacy?

MR. SNYDER: What you're describing in some ways is *Clapper* 2 in the Second Circuit which is the case that the ACLU brought. And they said, We actually were surveilled, and therefore we have standing. And the Second Circuit agreed in *Clapper* 2 because there was an obvious Fourth Amendment violation there.

THE COURT: Right. But in my hypothetical there was not a Fourth Amendment violation. Because you don't have a reasonable expectation of privacy in the garbage that you put out. But I don't think a court would say: I'm throwing this out on 12(b)(1) for lack of standing. A court would say: You don't state a claim under the Fourth Amendment so I'm throwing

it out on 12(b)(6). Another way of putting it is, you can assert an injury stemming from somebody searching through your garbage --

MR. SNYDER: I don't think there is an automatic injury and standing finding any time there is an allegation under a statute or the Fourth Amendment. And so I would say that in that hypothetical case I could see a court saying: If there is manifestly no expectation of privacy, then you don't have standing because there's no harm.

THE COURT: So can I put that another way? And I'm kind of agreeing with you, I think. Or at least showing you that I understand your point.

If it's super duper obvious that there's no expectation of privacy, no standing. If it's merely obvious that there's no expectation of privacy, standing, but failure to state a claim.

MR. SNYDER: No, I don't think that that subjectivity or nuance qualification is necessary. I think that if as a matter of law the well-pleaded allegations of the complaint manifest authorization, in the case of the SCA, manifest an understanding that there was no expectation of privacy in the garbage, then I think there is no concrete injury at all. And so I don't think it's an automatic rule, again. And whether it's obvious or not obvious, what's clear -- and I'm again getting ahead of myself -- is that these disclosures here which have been upheld by every court to ever consider them --

THE COURT: I understand your point.

Okay. Let me then turn back to Mr. Loeser, I guess, who was going to take me through --

Oh. I did want to ask one other question of you from this -- carryover from this morning -- before you take me through the --

MR. LOESER: Sure. Can we do one quick thing? It just corrects some factual statements --

THE COURT: Sure.

MR. LOESER: -- so the record's clear on this that Ms. Weaver's going to put on the record.

THE COURT: Sure.

MS. WEAVER: Thank you, Your Honor. I just wanted to address a couple of assertions that were made after we were going through the complaint and what the complaint alleges and does not allege.

And specifically, we do allege in the complaint in numerous paragraphs that Facebook is violating the privacy settings and its own privacy policies. So Mr. Snyder got up after we talked and said that we had admitted that they weren't.

What we think paragraphs 175 and 179 show is that they are violating user privacy settings. When they stripped that privacy metadata off the photos, they are violating those privacy settings.

THE COURT: Any other way in which they're violating the privacy settings?

MS. WEAVER: Yes. That's what I'm -- I apologize. In paragraph 169 -- I know we're not there yet, but it was a premise for some of the consent discussion.

The very last sentence there says -- this is dealing with the business partners: Facebook never told users it was sharing data with these third parties.

We have a cite there to the *New York Times* article that says this.

THE COURT: Yeah, but then we have the actual policy which seems to say something different. So we can get into that.

MS. WEAVER: You'll get into that. 298. Of course, the FTC consent decree required Facebook to -- at 298 ordered that Facebook prior to any sharing of a user's nonpublic user information, A, clearly and prominently disclose to the user, separate and apart from any privacy policy data use policy, statement of rights and responsibilities page, or other similar document, one, the categories of nonpublic user information that will be disclosed to such third-parties.

THE COURT: But you're not suing them here for violating the consent decree. Right? That's for the FTC to worry about. Right?

MS. WEAVER: Right. I think that's right. However,

we are saying that they did not abide by the consent decree. And when they are saying that they abide by privacy policies and disclosures, this is a point in the --

THE COURT: Well, maybe, as I said earlier, the way Facebook handled this was, you know, at a minimum, providing terrible service to its customers, right? And it may also have been a violation of the consent decree. But my job is not, I think, neither to decide whether it violated the consent decree or whether it provided terrible service to its customers.

MS. WEAVER: Okay. How about this? Paragraph 274 has the April 22 --

THE COURT: Which paragraph? Sorry.

MS. WEAVER: Sorry. 274. The 4-22-2010 version of the data use policy which again, you know, for periods of time we're saying isn't incorporated, but this is their policy that they are violating. Pretty far down in that paragraph, it's about four lines up from the bottom of 103: In addition, it will only be allowed to use that content and information in connection with that friend.

That was the -- we discussed this briefly about how API graphed 101, there were two pieces to not violating the policy. One, they're stripping the metadata off. And, two, an example we were using, they're not only using the photo just between me and Derek. They're obviously making it available to all app developers. And that had to be because it's the same platform

that allows apps to download all of the content and information that has to be true for all apps. For all under version -- Graph API, Version 1.0.

THE COURT: Let me go to paragraph 274 real quick.

MS. WEAVER: Okay.

(Pause.)

THE COURT: Okay.

MS. WEAVER: And I'm informed that I may be raining on my colleague's parade with this regard because he's going to address that in --

THE COURT: Okay.

MS. WEAVER: And then just a little bit of housekeeping. You had asked if we allege that any of our plaintiffs included messages and posts in the notification from Cambridge Analytica. And at paragraph 155 we do allege that for plaintiff Jarvimaki.

THE COURT: Okay. Hold on a second.

MS. WEAVER: It's the last sentence.

THE COURT: I don't know what that adds to what we've already discussed.

MS. WEAVER: Right.

THE COURT: It's a small number of people.

MS. WEAVER: Fine.

THE COURT: Right?

MS. WEAVER: I understand. Okay.

THE COURT: I don't know if this is a question for you or Mr. Loeser, but let me go back now to paragraph 124 of the complaint. This is a follow-up on our discussion this morning, from this morning, on the issue of the "public" settings. I just need to find it again. Sorry. 124. Okay.

Ah. Here it is. Okay. So we have this chart. And as I understand it, this chart reflects information that is available under the Graph API, Version 1.0, right?

MS. WEAVER: Yes.

THE COURT: And extended profile properties. You have user data and friends data.

So I asked you this morning if you set your privacy settings to "public," does that mean all of the information that the apps have access to, the third-party apps have access to, is information that some random member of the public could get by virtue of you having left your settings on "public"?

And the one thing you pointed me to as something that a random member of the public could not get, was the content of your messaging. But I thought we ought to look at this list and see if there is anything else on it -- and I assume it would be in the friends data column -- that a random member of the public could not get access to by virtue of you having your privacy settings on "public."

So what are all these things? What's "friends, actions, video"? Does that represent, like, that you liked the video?

Or does it represent that you watched a video? What does that represent?

MR. LOESER: Your Honor, our understanding is that all of these things here are things that app developers have access to but your friends do not. This is sort of the dossier background information.

THE COURT: But some of this stuff --

MR. LOESER: Some of it, obviously, is user likes and things.

THE COURT: So give me an example of something in that column where if you set your settings to "public" a random member of the public would not have access to that information regardless.

MS. WEAVER: May we put a pin in that and respond in a little bit? I need to look and think about it and I don't know off the top of my head. But we can get you an answer within --

THE COURT: Well, right. But then another issue is, you know -- getting me an answer is one thing. But then another issue is what's in the complaint and what's not in the complaint. Right?

And so you don't have allegations about what the default settings were, you don't have allegations about whether any of the plaintiffs had their settings on anything other than "public." And then regardless of the answer you give me, I don't think you have allegations in the complaint about what

these things represent.

So I think this is an example of kind of a growing list of potential deficiencies in the allegations in the complaint that potentially could be cured, I think. Or, you know, maybe they can be cured, maybe they can't. But at a minimum, it seems they could be improved. But anyway --

Okay.

MR. LOESER: Your Honor, just on that last point, this sort of -- there is a growing list. We get that. On some of what Your Honor is asking for, there's a decision that has to be made about the granular level of detail.

So, for example, we could obviously find out from our clients how they recalled they had their settings set. I don't believe they can access on Facebook -- and I could be wrong about this -- but I don't believe they can ask Facebook: Can you give me a history of how my settings were set? Maybe they can, but I don't think they can. But let's say they can and they can get that information. That's the settings.

There's also -- every time somebody posts something, they can make a decision as to whether it's private or public. And so you are talking about for every single one of these plaintiffs there might be thousands of different things, some of which would be set for "public" some for "private."

That's why the allegation in the complaint, you know, the plaintiffs intended for their information to be private; and

the inference that can be drawn from that, and it is a fair one, that they intended for their information to be private. Certainly, it would not be an inference in their favor to conclude that every single thing out of the thousands of things that was made available on Facebook they designated as "public." Because, again, the default was not "public." They would have had to designate that.

So we do have to sort out --

THE COURT: Well, except that's not in the complaint, either. But your point is a fair one. But it does appear that the allegations about each plaintiff's Facebook experience are pretty bare. And, you know, I don't know how much guidance I can give you about how much detail needs to be in there, but we we've identified some seemingly important points that are missing.

And that sort of brings me to another thought that I'll float now and we can talk about it at the end of the hearing. But I've been thinking about the way that I often handle securities fraud cases and other complex class actions at the motion to dismiss stage. Which is, you know, philosophically -- not just philosophically, but practically it strikes me that it's sometimes not helpful to have a hearing on a motion to dismiss and wait a long time for a lengthy written ruling from a district judge that nobody cares about -- except the plaintiffs and the defendants -- and then have another hearing

on a motion to dismiss, and wait a long time for another lengthy ruling from a district judge.

So this is often the point in the hearing in securities fraud cases and other class actions where I ask the plaintiffs: Have you -- do you think, after going through these last two and-a-half hours, that you have given your best shot at making allegations that would get past the standing issue at the pleading stage and get past the 12(b)(6) issue at the pleading stage? Because it might be that it's in everybody's interest for you simply to say: No. We can do better. And, may we have permission to amend our complaint now?

And I sort of think that that often is better for everybody involved to do it that way.

So anyway, we don't have to talk about that right now. Why don't you do what you've been wanting to do for a long time, which is walk me through the language and show me how Facebook has been misleading to its users or otherwise failed to disclose what's going to happen to its users' information.

MS. WEAVER: May I just make sure I understand the question about paragraph 123 so I can think about it and get back to you?

THE COURT: Yeah.

MS. WEAVER: You're asking if the user is at "public," is there anything in these categories that would have been nonpublic but given to app developers.

THE COURT: Yeah.

MS. WEAVER: That's exactly -- okay. Good. So I can answer that. The answer is yes.

THE COURT: And you can explain that to me. But it would also probably be useful to know if a user is at "friends only" is any of this stuff not accessible by a friend that would be accessible by a third-party app through the friend. Do you get me?

MS. WEAVER: I get the question. And I think I'm answering the right one. So that is the exact point of our case. I think I'm sharing "friends only" a photo, or I have something, and if I have posted a game activity and shared that with you by doing a post --

THE COURT: No. Sorry. I don't think you understand -- I'm not sure you understand the question.

So the first question is: Is there -- you know, if your setting is "public" and --

MS. WEAVER: The user setting is "public," or the friend?

THE COURT: Right. If the user's privacy setting is "public," is there anything that the third-party app can get through its interaction with your friends that a member of the public could not get? Other than the content of a Facebook message. That's question one.

Then question two would be, let's say somebody's setting

is at "friends only." Is there anything that the third-party app can get through your friend that your friend would not be capable of discerning about you? You know what I mean?

MS. WEAVER: I don't get the last one. So the user has downloaded the app. I am "friends only" with the user.

THE COURT: Yeah.

MS. WEAVER: Is there anything that is not limited to just us?

THE COURT: In other words, is there some --

So let me try to give you a concrete example that would apply to both questions.

Okay. We know that one of the things people do on Facebook probably more and more is they -- you know, they interact with other websites. Like I had a case couple years ago involving Zynga. It was a patent case, right? But I learned through that patent case that people go on to their Facebook page and they play FarmVille, or whatever one of Zynga's games, on their Facebook page. Right?

MS. WEAVER: Right.

THE COURT: So the question I'm asking is let's say the third-party app gets to you through one of your friends. Third-party app gets to you through one of your friends. Gets to your information through one of your friends.

I'm guessing that your friend may not be able to track when you are playing FarmVille on your Facebook page. I'm

guessing just the mere fact that this person is your Facebook friend doesn't mean they can track when you're playing video games on your Facebook page. And if I'm right about that, can the third-party app get that information by coming through the portal into the Facebook system through your friend.

MS. WEAVER: I believe so. I mean, it depends when they're accessing it at that moment in time. But let me check and confer and I'll get back to you.

THE COURT: Well, that; and then the question is is that in the complaint? Are the answers to these questions that I'm giving you in the complaint? Because I think it helps explain the extent to which there is or is not an injury and maybe is or is not a claim on some of these.

MS. WEAVER: Okay. Good. Let me think about it.

MR. LOESER: Okay.

THE COURT: I'm going to try to shut my mouth now for awhile.

MR. LOESER: Oh, please don't, actually. The most useful thing we can accomplish is answering the questions that were asked of us. And we really do want to do that.

THE COURT: So tell me what you want me to look at.

MR. LOESER: So first I'm just going to start by identifying the cases that I think are important to consider.

THE COURT: Oh, yeah.

MR. LOESER: And I will talk about the cases in the

context of my discussion of the disclosures and why it's not appropriate to consider them now and decide factual questions, but also why the disclosures are inadequate.

The first really important case that we think the Court should look at is *Opperman v. Path*, 205 F.Supp.3d 1064. at pincites 1072 through 1073, Northern District of California, 2016.

THE COURT: Okay wait. Hold on a second.

(Pause.)

THE COURT: Okay. *Opperman*, you said?

MR. LOESER: *Opperman*. And the reason why I'm starting with this case is there's a quotation from the case that really puts into context what we need to do when looking at these disclosures. And what the court said was: Consent is only affected if the person alleging harm consented to the particular conduct or to substantially the same conduct and if the alleged tort feasor did not exceed the scope of the consent.

In that case it was Judge Tigar, and he was looking at Yelp's terms of use. Yelp told users that Yelp could look at contact information to, quote, "improve the app's social networking function," but did not disclose that Yelp would upload the information to yelp.com, which is what the plaintiffs were complaining about. So you had conduct that was generally described, but it was not specifically described.

And because of that, the consent was inadequate.

THE COURT: Okay. Was that on a 12(b)(6) or --

MR. LOESER: That was on -- I believe that was on a 12(b)(6) motion. But I'll -- if I'm wrong about that, I'll later inform the Court.

THE COURT: Okay.

MR. LOESER: Then there's a series of cases that I think are important to look at that address this question of why consent cannot be determined at the motion to dismiss stage. Most of those cases are cases involving terms of use and data policies and things like that, and they involve other companies that are in the social media space, often cases against Facebook.

The first case is In Re: Google, Inc., Gmail Litigation. And that's 2014 Westlaw 1102660 at page 15, Northern District of California, 2014.

And in there, the particular pincite notes: The question of express consent is usually a question of fact where a fact finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals regarding the conduct at issue.

And I won't go through all these cases, but there's a few more that, basically, say the same thing.

The one thing of note that we just noticed over lunch in the *Google* case is it also addresses implied consent. It

addresses that consent and says regarding that -- and this is at page 16 in the Westlaw cite: The court now turns to implied consent. Implied consent is an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted.

THE COURT: So in other words, it sounds like the court in that case is thinking of implied consent in the way that I'm thinking about it, which is that for express consent you have a contract, and implied consent you don't have a contract but you have somebody that's been put on notice of what's happening.

MR. LOESER: Yeah. I would say in that case the defendants actually raised implied consent and it was briefed and considered, unlike this case. But I think that that's true, but the court also was evaluating -- it refers later to -- courts have consistently held that implied consent as question of fact that requires looking at all of the circumstances surrounding the events.

And so those circumstances would allow the Court, I think, to make the same determination about whether there was assent, similar to how a contract would be defined. But that's how that came up.

There's several Facebook cases. And I'm reluctant to --

I'll just say what they are then we'll move on to the rest.

THE COURT: *Cohen versus Facebook*, *Fraley versus Facebook*.

MR. LOESER: *Fraley versus Facebook*, which is 830 F.Supp.2d 785.

THE COURT: I mean, in those two cases it strikes me that they were -- that the -- it was just much less clear what Facebook was saying. And what Facebook was saying was subject to -- you know, much more amenable to differing interpretations than it's saying in your case. But maybe that leads us --

MR. LOESER: Yeah. And that's precisely where I would differ with Your Honor's analysis. Like in *Fraley*, the court was evaluating the SRR, the statement of rights and responsibilities, and terms of use, and got stuck on the same issue. Which is: Does the consent line up with the conduct? I don't know. To my mind, these cases don't involve disclosures that were any worse, frankly. They were just --

THE COURT: *Fraley* was the one -- that was the one about sponsored stories where they were -- the issue was whether Facebook had adequately disclosed that it would be using people's likenesses. Right?

MR. LOESER: To endorse a product. Yeah. But there were disclosures that -- you know, they came into court and they argued exactly what they're arguing here. These things clearly indicates this. The court stepped back and said, Well,

the plaintiffs certainly don't agree. And it's a factual question.

THE COURT: I think it's largely going to be just how clear or unclear is the language that Facebook used in this case. But before we get to that, do you have any other cases you want to make sure you bring to my attention?

MR. LOESER: The other you noted was *Campbell v Facebook*, 77 F.Supp.3d 836 at page 848. That's Northern District of California 2014.

Again, when you go into those cases what you will see is a dispute. There's language -- you can see what the language says. The plaintiffs look at it and are doing what I'm about to do and tell you why they don't think it's complete. The court stepped back and said, There's not an evidentiary record. Obviously, it can't be decided.

So those are the cases. And having gone through that I think I can just tick off. Again, before getting into the actual disclosures. Clearly, consent is something that's typically examined not at the motion to dismiss stage but on the merits.

It's also -- and particularly the way Facebook has raised the relevance of consent, they're raising it as a defense. And it's a defense on which they have the burden. And the case law is clear it has to be express in order to operate in the manner that they're asking you to have it operate.

Now, again, I'm putting aside the conversation about implied consent, but that's --

THE COURT: And the case on that point that is most important for me to read, you say, is the *Nguyen versus Barnes and Noble*?

MR. LOESER: *Nguyen versus Barnes and Noble* is very much on point for the issue of whether in fact the disclosures were part of a binding agreement. That case is determinative of that question.

The question as to implied consent, these other cases I think are more on point for the issue of if we should be evaluating that or not.

So let's go to the disclosures themselves. And I'm going to be referring to the slides that we have prepared.

THE COURT: Well, I'm fine looking at the slides as long as you --

MR. LOESER: They all have complaint citations in the paragraphs.

So the first significant problem with Facebook's disclosures is one that I'm not sure Your Honor wants to talk about, and that is business partners.

THE COURT: No, no. I do want to talk about business partners.

MR. LOESER: There is nothing -- and, again, putting your hat of -- I'm lining up the disclosure with the conduct,

can I see the conduct in those disclosures?

For business partners, Facebook did not tell people that even if they set their settings to "private" and in every way that they could, it was sharing information, user content information, with business partners. We only know that that is happening because the *New York Times* did an investigation, interviewed insiders, and it was revealed that this is happening.

The complaint discusses this at paragraphs 275 and 277. And so let's look at -- if you look at slide 16 -- and again, we're evaluating this language in the context of Facebook's decision to share user content information with dozens of business partners. And so if you go to slide 16, these are the kinds of things that Facebook said.

THE COURT: Okay. Could you give me a minute to get to the corresponding paragraphs in the complaint?

MR. LOESER: And this is paragraph 277.

THE COURT: Okay.

MR. LOESER: And I'm going to read what's in the paragraph and reflected in bullet 2 of the slide. I'm not going to bore you with reading all of these things. I think it would take too long. But just to give a flavor. Facebook says to users: Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook,

remove repetitive information from our user list, to process payments for products or services, to offer an online job application process, or to provide search results or links.

They say in these other statements that they provide information to service providers and to vendors. For example, on slide 17, which quotes from paragraphs 281 to 283, the first bullet Facebook says: We give your information to the people and companies that help us provide the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, and so on.

Now, what we've --

THE COURT: But in other words, this language makes it sounds like Facebook is kind of using almost subcontractors to perform some of the functions that -- the core Facebook functions -- as opposed to sharing data about users with business partners like Apple or whoever.

MR. LOESER: Right. Right. There's -- I don't know what these things mean. And that's the problem. What are vendors? What are service providers? It sounds like it's the people who, like, keep their lights on and bring them pizzas in the evening. I have no idea.

And here's what we learned about Facebook in the *New York Times* story: Internal documents show that the social network gave Microsoft, Amazon, Spotify and others far greater access to people's data than it had disclosed.

So this would be a great --

THE COURT: So this is what I was going to ask you. It seems like your allegations about how vague the disclosures are about sharing information with business partners or service providers are well taken, right? I mean, those allegations -- those disclosures are quite vague.

I guess one problem is -- it may not be your fault, but we don't have a good explanation in the complaint about the data that Facebook did share and what business partners did with that data. I'm not 100 percent sure how relevant that is what they did with the data.

But what is in the complaint -- so I'll ask you. What is in the complaint about what kind of data was shared with these business partners? What's in the complaint about who the business partners are? And what's in the complaint about what the business partners do with the data? And then if you have more information that's not in the complaint that you want to tell me that you could add to the complaint, you can do that, as well.

But first what's in the complaint on that?

MR. LOESER: What the complaint identifies are the facts that were revealed in the *New York Times* article.

THE COURT: So what is that? Show me in the complaint where that is.

MS. WEAVER: Paragraphs 169 through 174. 169 I just

referenced, it said: Those agreements permitted data sharing that was not subject to users' privacy settings. Second to last sentence. Moreover, Facebook never told users, et cetera.

170 discusses the how. And our understanding is that it's similar platforms to Graph API, Version 1.0, that allowed them to download it, but we don't know for sure.

Paragraph 172, Sandy Parakilas, who's the whistleblower, said developers had access to a friend's user data, and he said that these device makers, which are a subset of the business partners, were like apps in how they downloaded.

173 says they could retrieve relationship status, religion, political leaning, and upcoming events. And then tests by the *Times* show that the partners requested and received data in the same way other third parties did. Meaning, the app developers.

MR. LOESER: So on that one I would say we took the article, we took the facts that are disclosed, and we put them in the complaint. Of course, we kind of run up against the same problem that the world runs up against, which is Facebook has not been transparent. And they keep telling everyone that they're going to be or that they have been. And we keep learning things.

So we'd love to know more. We'd love to know exactly what was taken specifically from any individuals, but we don't have access to that information. So there's that.

So that's business partners.

The other area where these disclosures are really deficient comes from language in the statement of rights and responsibilities which we discuss at paragraphs 228 through 233 in the complaint.

THE COURT: Sorry. What paragraphs in the complaint?

MR. LOESER: 228 through 233.

THE COURT: Okay. Hold on. Give me one moment to get there.

(Pause.)

THE COURT: Okay.

MR. LOESER: And we've drawn out one particular bit of language in the slide 19. And this is the statement that: We do not give your content or information to advertisers without your consent.

So this is a big part of what we've heard from Facebook's counsel and what Facebook publicly says.

THE COURT: But doesn't that beg the question whether you consented to giving your data to third-party apps?

MR. LOESER: It does beg that question, but there's a more fundamental problem with the statement, which is that they do give information to advertisers without consent. And the way they do that -- there shouldn't be any dispute about the consent or the not consent. The way they do that is that they give information to apps, and those apps are often advertisers.

And so there's a disconnect between the disclosure. You're led to believe, Oh, they don't give it to advertisers without my consent. I haven't consented any advertisers. But they're giving it to these apps. And apps --

THE COURT: You mean the third-party apps requiring --

MR. LOESER: Yeah. Your example, FarmVille, is an app, and it advertises. So if you were concerned as a user about advertisers getting ahold of your information, you know, they are.

A better example is --

THE COURT: Sorry. Go ahead.

MR. LOESER: Cambridge Analytica. I mean, Cambridge Analytica was an advertiser. And users didn't consent in any way for their information to get in the hands of Cambridge Analytica.

THE COURT: But Facebook didn't give any information to Cambridge Analytica.

MR. LOESER: Right. They gave the information to Kogan, and then exercised no monitoring or control over what he did with it.

Something else that was not disclosed. That was another deficiency in these disclosures is they did not tell people that they did nothing to monitor what happened with this information.

So if you're a user, and you're trying to understand --

and this frankly understands the public outroar over Cambridge Analytica. People are asking: How did this company that creates some psychographic profile of me and is now trying to manipulate me on very important decisions in my life, how did they get my information? I never gave permission for this advertiser to get this information.

So there's no disclosure that would give anyone -- this is why people were so upset. There's nothing they could read --

THE COURT: Or, I never thought I was giving permission to -- I mean, that might be why they were outraged. Not because they never gave permission, but they didn't read the fine print carefully enough.

MR. LOESER: Is there a difference -- and I would interpret your question, or your statement to be, if the information given is so unclear you didn't know, is the information given?

THE COURT: Well, that gets back to another complaint that Facebook has about your complaint, right? Which is -- or, maybe -- I can't remember. Maybe Facebook doesn't raise this point. Maybe I'm just raising this point.

But, you know, on the issue of sort of the dearth of information about individual plaintiff's Facebook experience, you know, I want to know for each plaintiff did they read this? You know, did they misunderstand it? Or did they not read it? You know, maybe they don't remember. That would be totally

reasonable. But I want a little more about what each plaintiff's experience was with this.

MR. LOESER: Well, and here's why this case can be certified, which is the importance of answering the question you just posed. Because the standard would be an objectively reasonable person based upon these disclosures. And we will show to you that an objectively reasonable person would not believe that the disclosure authorized the conduct that actually happened.

THE COURT: Right. Although I'm not sure that helps you on the standing question, and on the question whether named plaintiffs have standing, you know.

MR. LOESER: Well, I think the named plaintiffs are objectively reasonable people.

THE COURT: Well, no, but I'm not sure. I haven't thought carefully about this. But I'm not sure it's enough for it to -- I'm not sure it's enough to apply the objective reasonableness test to determine whether a plaintiff had standing. I mean, if an individual plaintiff read this and understood it and disregarded it, you know, or if an individual plaintiff never read it at all, or if an individual plaintiff read it and didn't understand it, I mean, those are three different things that might have happened with an individual plaintiff and it might matter for standing.

MR. LOESER: Well, the good news for the case is that

so much information was omitted that we can answer the question both settings without, you know, picking an argument that gets us past today but eliminates us down the road.

So let's keep clicking through because I did want to --

THE COURT: Okay.

MR. LOESER: Another statement that there are disclosures discussed at paragraphs 371 and 376 of the complaint in which Facebook is indicating that it does not -- it anonymizes information so that individuals -- there's no way that, with the information shared by Facebook, that individuals could be targeted individually.

THE COURT: Which paragraph is that?

MR. LOESER: I have paragraphs 371 through 376.

THE COURT: Okay. Hold on a second. This is about the third-party advertising.

So your claim about the third-party advertising is -- I mean, does it rest on how much information advertisers have? Like, how good a job advertisers can do at targeting you?

MR. LOESER: Well --

THE COURT: I understand the argument about, Hey, Facebook was allowing this information to go to third parties without my consent. Right? But do any of your claims rise or fall on just how effective the advertising was or just how targeted the advertising was? Because if so, I don't understand that at all.

MR. LOESER: Well, here's the relevance of it. Again, we're looking at things that they told people. They told people that the information that's presented to apps is anonymous. Like you can't be -- when advertisers -- or, advertisers, I should say -- when advertisers, which is really a weird word to describe everybody in the world that does business with Facebook, but when they like come to Facebook and they want to advertise -- and, again, Cambridge Analytica calls what it's doing advertising because they're directing information at particular Facebook people -- people were led to believe that they could not be individually targeted. It was supposed to be anonymous information. However, the way this thing works --

THE COURT: Wait. You just said two different things. You said people were led to believe they could not be individually targeted. It was anonymous information.

That's a *non sequitur*. Right? You can be individually targeted even if the information is anonymous. In other words, it can be attached to a Facebook user ID as opposed to a name.

MR. LOESER: See, that's the problem. People didn't know that an advertiser -- like, people who got assaulted by Cambridge Analytica did not know, which is how a lot of people describe what happened, it was pretty offensive what they were doing. They were building a psychographic profile with information they got from content and information Kogan got

from Facebook, and they were developing information and then they were targeting specific voters. They could go after specific people. And that's a problem.

THE COURT: But is your claim that, you know, this information is not going to be used to target you? Is that what you are saying that Facebook said?

MR. LOESER: There's nothing about what they said to people that would allow them to understand that advertisers could single them out with complicated and misleading messages. That just wasn't -- people weren't told that. That's all I'm saying.

THE COURT: Well, wait a minute. I mean, it was clear from the disclosures that people could be targeted with advertising.

MR. LOESER: Not individually.

THE COURT: What does that mean "individually"?

MR. LOESER: They could collect -- if someone wanted to advertise to everybody who drives white Volkswagens, fine.

THE COURT: You could be individually targeted as one person --

MR. LOESER: As part of a group. You could be identified as part of a group that could be gleaned from your Facebook information.

But Cambridge Analytica didn't target groups. They identified particular voters and directed messages at them.

And so I guess we don't need to belabor the point. To me it just seems like --

THE COURT: What claim do you have, based on the distinction between those two things?

MR. LOESER: Invasion of privacy. So you did not know when you were using this platform that the kind of information being disclosed would allow what happened with Cambridge Analytica. You did not know that this information would go, somehow get to Cambridge Analytica, and they could do to -- they could do what they did to you.

That's why people are -- I mean, that's the reason for the uproar over Cambridge Analytica. They were identifying specific voters and seeking to influence their voting decision. And, you know, they did that because of the content and information they got from Facebook.

THE COURT: Okay. What about the -- I mean, the thing that this case was initially focused on was the extent to which third-party apps could get information about you through your friends. And so far you've rattled off like four different ways in which Facebook had failed to disclose things, and none of them are about that. I'm not saying they're not important. They are important. But what about the big one?

MR. LOESER: So here's the big one. And to set the stage for that particular issue. So Facebook has these profile settings and it has these app settings. The profile settings

are called profile privacy settings. And you go into these settings --

THE COURT: I think they're just called privacy settings.

MR. LOESER: They changed them multiple times. At one point they had the word "profile" in them, as well.

THE COURT: Okay.

MR. LOESER: And this is what the FTC got upset about. When you go in there and make those settings that you look at and say this controls the privacy and how I set it, there's also this other information that's in this data policy -- which again is not part of the contract, but it's over here (indicating) -- and it provides information about apps, and the ability of apps to share information. The ability of your friends to share your information via apps.

And one of the sort of structural problems that most privacy experts say is troubling about this, before we even get to the disclosures, and what the FTC said was troubling, is that it's not clear when you're in the privacy settings that this information will be disclosed via these app settings.

But more peculiar is that you can set privacy for yourself, but it doesn't control what actually happens to your information. You think that it's private, it only goes to your friends, but Facebook has made this decision to put into your friends' hands under these app settings the decision about

whether or not your information gets shared with people other than your friends.

THE COURT: I know. But it says -- but the various iterations say -- all, as far as I can tell -- say something to the effect of: You own all the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.

And it hyperlinks to both the privacy setting and the application setting.

MR. LOESER: So let's go to what it says in the data policy. This hyperlink. If you actually find that thing, which is not prominently displayed in some way that the FTC --

THE COURT: Okay. But the issue of prominence -- I mean, again, you haven't really made an argument, or much of an argument, about prominence. Or, you haven't cited a case to me that has said -- that stands for the proposition that even if the company discloses it perfectly accurately -- and this goes back to what we were discussing this morning, right? -- even if the company discloses it with perfect accuracy, it can still be a privacy violation if the disclosure is not prominent enough.

I think --

MR. LOESER: It's a great issue and a great question. Unfortunately, it's not the facts of this case. The FTC, when it evaluated these disclosures, did --

THE COURT: Why isn't it the facts of this case?

MR. LOESER: Because we've alleged that the information is not prominently displayed. It's hard to ferret out. It's misleading. And the FTC gave us a nice guide for how to do that, because it's exactly what it said.

But let's get to the -- so you mentioned the data policy, which is supposed to be -- and as counsel throughout their briefs they're constantly citing to the data policy as the Holy Grail of disclosure. It told everybody everything they needed to know.

So let's look at the data policy, slide 20 which -- quotes from the complaint at paragraphs 274 through 275. The data policy in effect from April 2010 through September 2011 says: If your friend grants specific permission to the application or website, it will generally --

THE COURT: Wait. Sorry. I want to make sure I'm on the right language. So which slide is this?

MR. LOESER: This is slide 20.

THE COURT: Okay. April 2010 to 2011.

MR. LOESER: Yeah. They change these things without giving notice to users.

THE COURT: I understand. I'm looking at the entire language. I prefer to look at the entire language rather than --

MR. LOESER: Unfortunately for me --

THE COURT: -- language that's been pulled out by

lawyers.

So when your friends use the platform? Is that where you are?

MR. LOESER: Yeah.

THE COURT: Okay. "If your friend connects with an application or website"? Is that the language you're wanting me to look at?

MR. LOESER: The language I'm reading is: If your friend grants specific permission to the application or website, it will generally only be to access content and information about you that your friend can access. In addition, it will --

THE COURT: Wait. Hold on. I want to see where -- I want to see where that language is.

So this is for the April 2010 to September 2011?

MR. LOESER: Right.

THE COURT: Okay. Hold on. Let me just find it.

Okay. So that starts: When your friends use platform. If your friend connects with an application or website, it will be able to access your name, profile picture, gender, user ID, and information you have shared with everyone. It will also be able to access your connections, except it will not be able to access your friend list.

MR. LOESER: Yeah. And if you keep going down the paragraph, there's the statement: If your friend grants

specific permission to the application or website --

THE COURT: Wait. Hold on. Let me just make sure I'm on the -- okay.

If your friend grants specific permission to the application or website --

MR. LOESER: -- it will generally only be able to access content and information about you that your friend can access.

THE COURT: Okay.

MR. LOESER: In addition, it will only be allowed to use that content and information in connection with that friend.

That is just, in addition to being extremely confusing, utterly misleading. And Cambridge Analytica is, again, the best example of why. Cambridge Analytica, 300,000 people downloaded this app. And, remember, this app and the way apps work on Facebook is it's the back door through which you get all the friend's data.

So they went from 300,000 to 87 million. It cannot possibly be the case that the information that they obtained only pertained to that person who gave that permission. You would have 300,000 people then. And that is a -- again, that is a huge issue and a huge reason why these disclosures --

THE COURT: So that sentence is definitely vague. No doubt about it. So let's look at the next sentence and see if

that helps explain it.

For example, if a friend gives an application access to a photo you only shared with your friends, that application could allow your friend to view or print the photo but it cannot show that photo to anyone else.

Sort of nonsensical.

MR. LOESER: Does it mean anything to you?

THE COURT: We provide you with a number of tools to control how your information is shared when your friend connects with an application or website. For example, you can use your application and website's privacy setting to limit some of the information your friends can make available to applications and websites. You can block all platform applications and websites completely, or block particular applications or websites from accessing your information.

MR. LOESER: Yeah. So you've just told people that when they go through these app things, Hey, don't really worry about it because if your friend gives access to information we can only use it with regard to your friend.

THE COURT: Okay. Then what do you say in the complaint about that? Take me back to the part of your complaint that explains why that's misleading.

MR. LOESER: What the complaint says about this, and I'll struggle to find the actual cites unless somebody can hand them up to me.

THE COURT: 271? Hold on. Let me go to it.

MR. LOESER: And, you know, just for the record, Your Honor, preparing for these hearings takes a tremendous amount of work. And this team of people back here do an amazing job equipping us with the information we need to answer these questions.

THE COURT: Appreciate that.

Okay. Paragraph 271. Go ahead.

MR. LOESER: Facebook made it difficult for its users to understand that third parties were constantly vacuuming up their content and information and that Facebook was not monitoring what they did with it.

You know, Your Honor, there are actually dozens of paragraph references to the way app settings were unclear and sort of lull people into believing that they had nothing to worry about because the information wouldn't be widely shared. And we could -- we could assemble all these things.

Actually, a point I was going to make at the beginning. As to all of these questions, and I fear we're actually going to run out of time before we've really directly answered the questions posed, and it might be helpful for us to submit some briefing on those questions in which we really could answer them. We'll leave that up to Your Honor to decide at the end of the day if it's necessary.

But there are many, many references in the complaint. And

as I continue to talk, I'm sure more numbers will be assembled. But that is a fundamental failure of these disclosures and it's repeated in a variety of ways.

THE COURT: But as to that particular sentence, I kind of understand what you're saying, but other than reciting that sentence in the complaint I'm wondering if there's anything in the complaint about explaining how people were misled by that. I mean, maybe your answer is, Well, it's self-evident, so we --

MR. LOESER: But there are allegations in the complaint. And, unfortunately, I can't cite them off the top of my head but we can provide them to you.

But the tenor of the allegations is that because of the way this information was presented, people did not know that all of their information was being revealed this widely with these apps. And had they known that, they could have considered it. It's recited in the claims, as well. I mean, it's something we kind of keep coming back to over and over again.

THE COURT: Okay.

MR. LOESER: So, you know, about the particular --

THE COURT: So the issue is not that -- at least based on the way you've described it now -- the issue is not with the failure to disclose that apps would have access to this information through your friends. The issue is with the failure to disclose that apps would be able to use it in ways

beyond using it only in connection with that friend.

MR. LOESER: There's a couple different ways this disclosure, and specifically the disclosure that you've put your thumb on in your questions, about the app settings and the discussions specifically in the data policy about the app settings, doesn't provide users with sufficient information about the sharing of their data that will occur. Because of the lack of full disclosure, it made it appear as if less information of theirs would be shared. That's one.

Two, because of the structure -- and this is what the FTC --

THE COURT: Well, how is that? It appears that less of their information would be shared with third-party apps than was disclosed? So it's not --

MR. LOESER: What they flat out said was they would only use the information with regard to the person who shared it. So I hear what you're saying. I should be a little more precise. It wouldn't be disseminated as widely.

THE COURT: Okay. So it's not the disclosure of the information that you're taking issue with. It's the use of the information and the wider dissemination of the information than what was represented in the disclosures.

MS. WEAVER: Your Honor, I think it's both. And if I could just -- and we had divided things and you're getting a little bit into standing. And so let me just express why --

where we see the harm here.

If you go next to paragraph 276 in the complaint --

THE COURT: I don't know if this is only about standing. I mean --

MS. WEAVER: Right. No. It's about everything. But it's with the conduct and what happened and how it's perceived. How it was described to users, and what actually happened to them. And there's a delta there.

So paragraph 276, the disclosure says: When you share and communicate using our services you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your friends, or members of a group. Likewise, when you use Messenger you choose the people you send photos to or message.

That, we would argue, is false and this is why.

If you conceive of Facebook as a two-tiered platform. And there's one platform where users interact with each other. And it's on those -- that -- we'll call it the user platform, that's where the privacy controls operate.

And so when Facebook is saying: Oh, you control your audience, all the user is thinking about is the other people on the platform. But there's a second layer that was going on that people did not understand and was not clearly explained. That -- all of this Graph API, the platforms that were built

for app developers, was operating underneath.

And what it meant, really -- and not to make a television reference -- but this is kind of like Westworld. There are two realities going on at the same time. So I think I'm having a private interaction with my friend, and instead there's an army of companies who are reviewing that interaction, analyzing it to figure out how to target me. They are getting realtime responses. They're going to Facebook and saying, Hey, we want to ping them. And Facebook is letting them know how you respond.

So what's so offensive about it, and what's so troubling about it -- and really it's a public policy problem for all of us -- is that it's a one-way mirror. So I'm standing in this room and I'm getting these messages --

THE COURT: But rhetorically, that all sounds great, but the reality is that notwithstanding the statement that you just identified from the complaint, you choose the audience who can see what you share. I mean, that is qualified by other statements that Facebook makes along the lines of, you know, these third-party apps can get information from your friends about you. And your friends can choose to allow third-party apps to access all this information about you. And whatever your friends can see about you, these third-party apps are going to be able to see about you unless change your settings.

MS. WEAVER: No. Even if you change your settings.

THE COURT: Well, no. You can change your settings. But it also discloses. The point is that it discloses that you can change your settings to significantly limit the amount of information that friends can share about you. But there is some information that your friends will always be able to share about you unless you completely turn off this app setting.

MS. WEAVER: That's for apps.

THE COURT: But the point is that it's disclosed.

MS. WEAVER: And for business partners, there's nothing you can do to prevent business partners from getting it. And if you think that the disclosure about service partners --

THE COURT: Right, but we're talking about apps now. We're talking about the apps. So I do understand. And I will tell you that I hadn't adequately focused on this one sentence can only use that contact and information with your friend, right? That is an issue. I understand.

But putting that aside, I just -- with respect to the apps -- and maybe that one sentence is enough for you. But with respect to the apps, if you're merely talking about what Facebook said and you're not talking about how prominently Facebook made the disclosure, but just the words that it used, it seems like the words contain everything.

You read those words and -- you know, you know, look, let's face it, nobody takes the time to read those words. But

the law sort of presumes that people reads the words, generally speaking, which is why I asked about whether the prominence of it matters. But if you read the words, you come away knowing that even if you limit your settings so that you're sharing only with friends, these third-party apps can communicate with your friends and get all of the information that your friends have access to unless you further change your settings. And then even then, you can further change your settings, but if you want to have a meaningful Facebook experience, apps are still going to get some subset of information about you. All of that seems to be disclosed.

MR. LOESER: Your Honor, now you're getting tag teamed. Hope that's okay.

But I would suggest to you that when the FTC -- and we're not litigating the FTC's case. But when we're evaluating whether these disclosures, whether they're content, which is what we've been talking about, is sufficient and whether their placement which -- their prominence is sufficient, the FTC looked at the same things we're talking about and said it's not sufficient. The content is not sufficient and the placement is not sufficient. And it told them you have to fix it.

THE COURT: When did the consent decree get entered into?

MR. LOESER: 2012.

MS. WEAVER: It was started in 2011.

MR. LOESER: Their complaint was filed in '11, it was filed in '12. And I only raise that because your Honor is struggling with --

THE COURT: Well, it must have satisfied the plaintiffs in that case. I don't know who the plaintiffs -- well, was it the FTC that was the plaintiff in that case?

MR. LOESER: The FTC sued them, and then there was a consent decree requiring them to do things which --

THE COURT: So presumably, the FTC was comfortable with the changes that Facebook had made.

MS. WEAVER: Well, they entered a consent decree, but they have opened the investigation again.

MR. LOESER: It's ongoing. And government shut down for awhile, so who knows what's really happening.

But my point -- I don't want to litigate the FTC's case. They have their own. My point is only here we are at a motion to dismiss. You're stuck in this spot of having to evaluate the sufficiency of the complaint. We're telling you there are some real factual questions here that can't be decided. And, when the FTC looked at the same kind of thing what they concluded was that it was not sufficient.

So it seems like it would be maybe a bridge too far to look at these same disclosures now and say as a matter of law they're sufficient, when a federal agency has looked at them and said they're not.

And there's some very specific things that Facebook was supposed to do and didn't do. And those things have to do both with the content and with the prominence of where that information is presented.

THE COURT: Okay. Is there anything else you want to tell me -- focus me on with respect to the adequacy of the disclosures?

MS. WEAVER: I would just mention also with disclosures -- and I'm sure Your Honor's aware of this -- we're looking at documents in hard copy here. Most people are downloading these things on their phone. And so as to your point about prominence, it is a lot to expect these fine print legalese documents, with different moving parts and apps, we've got all these different settings to protect yourself, and even that doesn't work. And the net-net is that if you wanted to protect yourself, and those privacy settings meant anything, you needed to not have any friends. And that's not the product that Facebook was selling.

THE COURT: So just -- I apologize, because I know I've sort of asked this question a number of times. But are you aware of cases -- like let's say, for example, cases under the California constitution's privacy provision or the common law privacy tort that talk about the need to make a disclosure more prominent as the privacy interest becomes more significant?

MR. LOESER: You know, Your Honor, A, we'll research that question and try and give you specific cases.

THE WITNESS: Where I have seen cases that discuss this issue of conspicuousness, prominence, are the browse-wrap, clip-wrap cases. And the *Nguyen* case I really encourage Your Honor to read. I would read it in the context of the arguments Facebook is making. They're making a contract argument based on the data policy. And under that case, the argument fails for them.

THE COURT: Okay. We have a couple other topics I want to discuss, but I think it's good to switch sides now for a little bit.

MR. SNYDER: I want to try to bring us back to the law and to the text of the complaint and the applicable disclosures.

So first let me start with the law just to frame the discussion, Your Honor, and then I'll afterwards talk about business partners and -- but let me start with first.

The cases, a lot of which counsel is referring to about the internet, are old cases. This is really settled law. The backbone of the internet and our digital economy, which is increasingly our national economy, is these disclosures and agreements. And courts have reviewed them and, in fact, the Ninth Circuit just in December reviewed Facebook's and affirmed the district court's dismissal on the merits of a complaint in

the *Smith v. Facebook* case decided December 6 of 2018. And said that: In determining consent, courts consider whether the circumstances considered as a whole demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization. We, of course --

THE COURT: Considering the circumstances as a whole seems to include prominence. Right?

MR. SNYDER: Well, I don't know about prominence. I think it is a question of clarity, and like in construing any disclosure, whether it is clear and on point. And we believe that the disclosures -- and I'll go through them very quickly -- were clear, blunt, on point, meaning covered the very conduct complained of. What's notable about the complaint, of course, as Your Honor pointed out, is there is no allegation that any plaintiff had any difficulty understanding, reading, finding, navigating or assenting to the disclosures. No named plaintiff. They have generic broad sides against our disclosures, but they don't even allege that any named plaintiff believed there was an ambiguity. And, of course, their belief wouldn't make it so, but it's not even alleged.

But just as in *Smith* where the court ruled a reasonable person viewing the disclosures there, which involved cookies and tracking and collection of user information and they ruled without any hesitation affirming a 12(b)(6) dismissal in that

case, that Facebook maintains the practices of, A, collecting it's users' data from third-party cites and, B, later using the data for advertising purposes. And knowing authorization of this practice constitutes consent.

And, of course, Facebook's terms and conditions have been upheld repeatedly by courts, in addition to the Ninth Circuit a couple months ago. And we cite those in our brief.

But what we can walk Your Honor through quickly, and of course counsel did not read the most important disclosure of all which is crystal clear, on point, and dispositive, which is where Facebook told users that friends could share their information with apps. And that's at 275 of the complaint.

THE COURT: Wait. Hold on. I'm sorry. Let me pull it back up.

Hold on. Sorry. Paragraph what?

MR. SNYDER: 275. And before I begin, Your Honor, you and counsel spent time -- about ten minutes or more -- talking about disclosures from 2010. And, of course, the This is Your Digital Life app didn't commence until 2013. So what counsel did not read to you was paragraph -- allegation 275, which was in effect at the time of the Cambridge Analytica and Kogan events.

THE COURT: Right. But somebody who joined Facebook before then, there would be no reason for them to have read this, right?

MR. SNYDER: No. But the law is clear, Hornbook law, that by agreeing to a user policy and continuing to get the benefit of a free service, you assent to future revisions of the policy. I don't think there's any controversy there.

And, you know, we would respectfully disagree --

THE COURT: No matter what the revision is.

MR. SNYDER: Well, so long as the revision is clear and lawful, sure.

And, Your Honor, we do dispute the notion that users blindly click on and don't read privacy settings. I don't have it -- the Court might be able to take judicial, but of studies of how millennials and others are very careful and assiduous about understanding privacy and the like.

So if you look at this disclosure here, it's difficult to find a clearer enunciation --

THE COURT: I mean, I think you just kind of helped them make their point that maybe this isn't the type of thing that's amenable to resolution on a motion to dismiss.

MR. SNYDER: No, Your Honor, to the contrary. The Ninth Circuit just affirmed the district court dismissal based on Facebook's --

THE COURT: That was a different disclosure of a different policy.

MR. SNYDER: Right, but I haven't walked through, Your Honor, yet why this policy fits like a glove --

THE COURT: Okay.

MR. SNYDER: -- what is alleged here. Like a glove. So, Facebook told users that their friends could share their information --

THE COURT: You're looking at the disclosures from paragraph 275?

MR. SNYDER: Yes. And it says: Controlling what is shared when the people you share with use applications.

THE COURT: Can you show me where in that paragraph you are?

MR. SNYDER: Yes. I'm in the first "just when." The very first --

THE COURT: Okay.

MR. SNYDER: Just when you share information --

THE COURT: "Just like when."

MR. SNYDER: Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared.

THE COURT: Okay. Stop there. That sentence is misleading. That sentence, at least in isolation, is misleading. Because there's a big difference between sending an email to somebody that might be re-shared by the recipient, and having your information packaged and given to a third-party.

MR. SNYDER: Your Honor, it's not misleading when you

read the full context. And like any disclosure, you can't take --

THE COURT: Okay. But full context is the first sentence you read, in and of itself, is misleading.

MR. SNYDER: I respectfully and strongly disagree.

THE COURT: You better do a good job of clearing it up.

MR. SNYDER: I respectfully and strongly disagree that there's anything about that misleading.

THE COURT: So you think the risk -- you think the risk of sending somebody an email, the privacy risk of sending somebody an email, is as great as the privacy risk associated with allowing third-party apps to gather all of your information from your friends.

MR. SNYDER: Right now this disclosure's not talking about third-party apps. It's talking right now about the general notion that what you share on Facebook with third parties, friends or others, can be re-shared. It's a very banal statement. It's not conversational. It's --

THE COURT: It can be shared, including the games, applications and websites.

MR. SNYDER: Right. But then it goes on and says what it means. This means that if you share something on Facebook, anyone who can see it -- anyone -- can share it with others, including the games, applications, and websites they use.

Your Honor, that's exactly what counsel just said was scary and pernicious and Westworld.

This is a clear disclosure that if you share something on Facebook, it can be re-shared. Truthful. Not misleading. How can it be re-shared? This means that if you share something, anyone who can see it, meaning your friends or the public -- but let's say just friends only -- can share it with others, including the games, applications and websites they use.

This is a clear disclosure that if you share something on Facebook and your settings are to "friends only," your friends can share it with the companies that host games, the applications that you use, not in a two-tiered platform, in a single holistic platform called Facebook, and the websites they use.

This is crystal clear.

It goes on to be even clearer. It says, if you go down a little bit -- I'm not going to read the whole thing. But it says: If you have made that information public. If you have made that information public, then the application can access it just like anyone else. But if you shared your likes with just your friends, the application can ask your friend for permission to share them.

And then it goes on to say: We've just told you that you should have no expectation of privacy with respect to third-party websites, third-party apps, third-party games if

you share anything on Facebook with anyone. But -- there's no trickery. There's no intrusion.

You are in control, user. Because most of the information other people share with applications you can control using your apps and websites hyperlink, easy to access. But these controls not only limit access to your public information and friends list. Elsewhere it says you can shut off your apps entirely.

And so it's difficult to imagine clearer disclosures that cover the conduct at issue here. And Facebook's terms and conditions have been upheld repeatedly by the courts. The Ninth Circuit just did it, affirming a dismissal. And the disclosures here fit the conduct here just as, maybe even -- just as the disclosures in *Smith* fit the conduct there.

THE COURT: Could I ask you a question about that? I'm looking for -- so I'm looking in the language in paragraph 275 for the sentence that I was speaking with plaintiffs' counsel about and I'm not finding it. But that language is in the previous paragraph discussing the April --

MR. SNYDER: It is there, actually. It's not the same, but it's a little bit the same. And it's on the last paragraph before 276.

THE COURT: Okay. Let me see that.

If an application asks permission from someone else to access your information, the application will be allowed to use

that information only in connection with the person that gave the permission and no one else.

So talk to me about that.

MR. SNYDER: That's correct. So that language was true as to Kogan; meaning he and other apps were supposed to use friend information only to enhance the social experience between that user and friend. That was the personalty test.

What happened was he, in violation of our platform policies, then sold or transferred that data to Cambridge Analytica, which was not allowed by our policies, and which by the way -- not that we were happy about it -- we warned users in -- this is Exhibit 45.

THE COURT: I mean, I know that he sold that information to Cambridge Analytica in violation of your apparent policies. But was Kogan using it only in connection with the person that gave the permission and no one else?

MR. SNYDER: Yes. Yes. Until he transferred it to Cambridge Analytica, yes.

But here's -- but, Your Honor, I want to go back to -- I'm not avoiding this paragraph, but I don't understand how any fair reading of what I just read can lead to any conclusion other than that Facebook's policies, disclosures informed users regarding each and every one of the alleged harms at issue.

Let me go to the device manufacturer, which is truly, I think, been mischaracterized in the colloquy you've heard.

Actually, let me go back to the first point again just because counsel did talk about a case. The Ninth Circuit case. I believe it's N-Y-U-Y-E-N -- or, N-G-U-Y-E-N. And the terms of use -- that was an arbitration case, as many of these are. And the terms of use with the arbitration provision were not called out at all but were linked at the bottom of the page where it said "policies:" So the court wasn't happy with that.

That's completely off point to this case. Because here if you look at paragraph 264, plaintiffs admit -- and again, I think this is fatal to their arguments -- that under the sign-up page for Facebook there was an express statement that users by clicking "sign-up" had read and agreed to the terms of use and the privacy policy.

THE COURT: But that wasn't for the entire class period, right?

MR. SNYDER: Was that for the entire class period?

THE COURT: I don't think so.

MR. SNYDER: I believe it was, Your Honor. But I can answer -- I can clarify it.

And I'm not aware of a single case, Your Honor, certainly in the Ninth Circuit, but anywhere, a decision striking down Facebook's agreements as insufficient for -- insufficient for assent. And, I'm not aware of a single case that reads our policies and says that they weren't crystal clear as to conduct where there is no delta -- to use counsel's phrase -- between

the conduct and the disclosures. And if we want to go to the device manufacturers, the same conclusion obtains there.

Oh, and in all the other Facebook cases quoted, the *Cohen* case, the *Campbell* case, that involved the court ruling that the disclosures didn't cover the challenged conduct, as Your Honor --

THE COURT: Or, might or might not have.

MR. SNYDER: Or might not have. Right.

And so if you look at the so-called device manufacturers or business partners, what's going on there is at paragraph 170 in the complaint. Essentially, before --

THE COURT: Hold on. Let me get to that real quick.

MR. SNYDER: Let me just back up for a minute before I direct your attention to the complaint.

Before there were apps for different devices in the early days -- I don't know if Your Honor recalls -- but if you wanted to access Facebook on your BlackBerry or Android, there wasn't an app for that. And instead, the device manufacturers or partners built a Facebook-like experience. It was pretty rudimentary and crude, not as nice and effective because it wasn't a Facebook platform. It was a platform that was built by a partner to host a Facebook-like experience.

And in order to facilitate that benefit to the user, the user consented to exactly what paragraph 281 of the complaint states. And --

THE COURT: 281?

MR. SNYDER: Yeah.

THE COURT: Wait. Hold on. Give me a second.

MR. SNYDER: Sure. And in 281, the top of page 108, so it's actually the first quoted language after "service providers," it says: We give your information to the people and companies that help us provide the services we offer. For example, we may use outside vendors to help host our website, serve photos, and videos. In all of these cases, our partners must agree to only use your information consistent with the agreement we enter into with them as well as this privacy policy.

And so what that's saying is we, to enable you, user, to enjoy Facebook on devices, mobile devices -- in the early days before the Facebook app was ubiquitous -- we are going to share your information with our partners to do what? To help host our websites, serve photos and videos.

So what's ironic about this allegation is that this was a disclosed benefit to users so that they can enjoy a Facebook-like experience on their mobile devices. And on paragraph 170, the plaintiffs acknowledge that the purpose of these partnerships was to facilitate, as I said, a Facebook -- availability on mobile phones and other devices with other operating systems.

And so here, A, there's disclosure which we think is

sufficient. But, B, we run headlong into the standing problem. Because our standing argument, with respect to this allegation, doesn't depend solely on consent, but also on the complete absence of any concrete harm. Because all that's happening here is to benefit the user, that user is getting to enjoy Facebook on a mobile device.

That's a benefit. That's not a harm.

THE COURT: But it sounds like, at least if the allegations of the complaint are to be believed, that that bled into something else over time. And what the complaint alleges in paragraph 284 is that the language changed in January 2015 and read this way until April 2018: We transfer informing to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our services are used, measuring the effectiveness of ads and services, and providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations.

I mean, it sounds like that would not include third-party apps, but it still reads as, kind of, our people who are helping us provide our services.

MR. SNYDER: That's exactly, though -- it says "partners," Your Honor. I don't know how to be -- I don't know how they could have been clearer other than listing 100

different companies. But they say: We're going to give your information to outside vendors to help host our websites, and our partners have to agree to use your information.

And the point here, Your Honor, is --

THE COURT: But it's interesting like if you compare this language to the language about the third-party apps, right? In a lot of ways the language about the third-party apps I thought was very good, you know, putting aside the question of how prominent it was, or whatever, how hard it was to get to. Because it said, you know: We are going to do this. What this means, for example, is this might happen or that might happen or this might happen.

Here, when we're talking about business partners, I'm not seeing any: Let us explain to you what we actually mean. Hey, this language might be a little vague, so let's explain it to you. For example, we -- if you use your Facebook app on your Android, Android is going to get your information. And here's the information that Android is going to get.

There's no explanation of that.

MR. SNYDER: It doesn't say that and there is no further explanation. But we believe I guess, one, and contend that is sufficiently clear and on point.

THE COURT: Well, what if I want to opt out? What if I don't want -- what do I do? So let's say I read this and I'm somehow able to discern that one of the companies -- let's say

Microsoft. Let's say I'm using it on my desktop, or whatever. And Microsoft is one of the companies that Facebook shares my information with by virtue of my using Facebook on my desktop.

Let's say I'm somehow able to discern that from this language. Which is doubtful. But if I am, where are the instructions that tells me how I can avoid Microsoft getting my information? The kind of thing that is in the disclosure on the third-party apps.

MR. SNYDER: I agree with that, Your Honor. But I guess my point is that even if you believe that this disclosure could or should have been as clear as the other disclosure, there are two other independent reasons why it doesn't matter for standing purposes. One, there's no allegation that the business partners did anything wrong with the info.

Every other --

THE COURT: Why does that matter? I don't see how that matters.

MR. SNYDER: Because every standing case -- every standing case finds that there has to be a concrete injury associated with the alleged act. And here --

THE COURT: But the disclosure of your private information without your consent is an injury.

MR. SNYDER: Consistent with your assent to share information broadly on the platform with friends and with others. So, again, there's an absence of a privacy interest

here, Your Honor, because we're not dealing with an intrusion from a hacker --

THE COURT: But none of it depends -- if you did not consent to your private information being disclosed to a third-party -- you argue here that they consent -- but if you did not consent to your private information being disclosed to a third-party, surely you are not telling me that if that private information is disclosed to a third-party there is no injury unless somebody does something wrong with that information.

MR. SNYDER: No. But given the consent here that was broadly given in numerous contexts, there is no concrete harm in the incremental sharing with these device manufacturers. So even if you find the consent is not sufficient, that incremental sharing to facilitate an advantage and benefit for the user so they can enjoy their Facebook on a different operating system, does not result in a real world actual concrete harm under our --

THE COURT: Yes, it does. I mean, it depends again -- I might not -- I may not want my private information shared with a third company. And unless you adequately disclose to me that you're sharing my information with a third company, and unless you adequately disclose to me the costs and benefits of that, then that's an injury.

MR. SNYDER: I respectfully --

THE COURT: It doesn't matter what the third party does with it.

MR. SNYDER: I respectfully disagree because you have to look, Your Honor, at the context of the sharing. And here there is no non-speculative actual injury, for sure. There's only a --

THE COURT: The injury is in the disclosure of private information.

MR. SNYDER: There has to be a concrete harm associated with it, Your Honor.

THE COURT: Okay. So Facebook is standing in court right now -- Facebook is standing in court right now and telling me that the disclosure of its users' private information to a third company is not injurious unless the third company does something bad with the information.

MR. SNYDER: Your Honor, I keep on pushing back on that. With consent. With consent.

THE COURT: That begs the question --

MR. SNYDER: Which is why even in some hacking cases --

THE COURT: But you keep saying, No, no, no. You're moving the goal line. Because what you've said to me more than once here is even without consent, there's no injury here because there's no allegation about what the third parties did with the information.

MR. SNYDER: I'm sorry. I either misspoke, or you misunderstood me.

Even if you find this one specific consent is not as fulsome as you want, the fact that the users consented broadly to sharing their information with friends, with third-party apps, with games, and with all manner of third parties, means that they don't have an expectation of privacy with respect to sharing to facilitate the use of their Facebook on another platform for their benefit, because there is no actual or imminent injury. And so there's no actual injury. We know that. And, therefore, there has to be a credible risk of future harm.

THE COURT: That gets back to your -- they don't have an expectation of privacy because they've consented to the sharing of this information with all these other folks. And so even if they didn't consent to the sharing of information with Microsoft, there's no injury from an Article III standpoint.

MR. SNYDER: No injury unless you can plausibly allege a credible risk of future concrete harm. And where you have the third-party manufacturers ios platform providers adhering to confidentiality and the Facebook privacy policy, I don't see the actual harm. I see speculative harm. I see a *Clapper*-like possibly one day the companies will do something with it. But what's fascinating is we've had three, four years now of this alleged harm with the sharing with partners, and there's not a

single allegation of an actual injury. And there's not a single --

THE COURT: The allegation is -- well, they have other allegations about economic harm and all that stuff, which I'm not buying. But the allegation is that I was injured because my private information was disclosed.

MR. SNYDER: Right.

THE COURT: You keep saying there needs to be something else bad that happens --

MR. SNYDER: No.

THE COURT: -- with that information.

MR. SNYDER: I'm saying that where there is broad consent, understanding that you're not keeping your information private, that you're sharing it broadly with third-party games, third-party applications, where you're told in black and white in this paragraph 281 of the complaint that we are going to give your information to others to host websites and that they're going to adhere to our agreement, there is no injury in fact of any kind. And there is sufficient disclosure to both cover the conduct; and in any event, certainly no concrete harm.

THE COURT: See, I think you have a point. You keep distracting me by trying to make it a standing point. I don't think it's a good standing point. But I think you have a point if you're talking about whether they've stated a claim on the

merits with respect to the disclosure of sharing information with business partners.

MR. SNYDER: Yes.

THE COURT: Because maybe you would say, based on the totality of this --

MR. SNYDER: Correct.

THE COURT: -- given that they consented to disclosure of this information to all these other people, they no longer have any reasonable expectation of privacy in it.

MR. SNYDER: Yes. And --

THE COURT: How does that work for the Stored Communications Act claim?

MR. SNYDER: Well, the Stored Communications Act you need --

THE COURT: Because you need consent. You need their consent to disclose it to Microsoft.

MR. SNYDER: Right. Or, you need -- for Article III standing under the SCA you need concrete harm, and there's no concrete harm.

THE COURT: Forget about Article III standing. On the merits, for the Stored Communications Act, you need their consent to disclose it to Microsoft.

MR. SNYDER: And we believe that consent is affective, valid. And in paragraph 281. And in the -- to Your Honor's point of implied consent, what does the user think is happening

when they open their BlackBerry and get served on BlackBerry a Facebook-like experience that they know isn't Facebook, they know is BlackBerry creating a Facebook-like experience?

What -- how can we possibly say that the user is injured or hurt when by volitionally going on to their Microsoft desktop or their BlackBerry and accessing that service provider's operating system, and lo and behold there is their Facebook information? What do they think is happening?

THE COURT: Since I asked you the question about the Stored Communications Act, can I ask you a couple other specific questions about that claim?

MR. SNYDER: Yes. And you know, Your Honor, every time you take me to 12(b)(6) I'm taking you back to --

THE COURT: I understand. But it might be to your detriment on occasion.

MR. SNYDER: Yes, Your Honor.

THE COURT: So on -- there's an argument you didn't make, and I was wondering why you didn't make it for the Stored Communications Act.

Which is that the statute says that a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication.

I might have expected you to argue that -- I mean, maybe like politically you can't make this argument, or from a

business standpoint you can't make this argument -- but I might have expected you to argue that it's not Facebook that is knowingly divulging any information to these third-party apps. Facebook is giving access to the platform to these third-party apps, but it is my friends that are knowingly divulging my information to these third-party apps. And so if anybody, it's my friends who violated the Stored Communications Act by giving the apps permission to get the information.

MR. SNYDER: And, of course, the Stored Communications Act only governs and prescribes conduct by service providers. So I don't think we would argue that the Stored Communications Act governs what the friends do.

THE COURT: The friends do.

MR. SNYDER: What the friends do. But I would say that, you know, clearly going back to your question, too, the Stored Communications Act does not protect the further sharing of communications as alleged here. And it doesn't give the consumers, certainly, the right to sue in these circumstances. It simply gives a private right of action to anyone who is aggrieved by a violation of the statute. And the Supreme Court has long held that the statutory reference to any person aggrieved doesn't reflect any congressional judgment about what kind of injuries are sufficient to confer Article III standing.

THE COURT: On the merits of the Stored Communications Act claim, the exception is that, you know, you can disclose

this with the lawful consent of the originator, or the customer, or whatever it is.

MR. SNYDER: Or subpoena or court order.

THE COURT: Lawful consent. Lawful under whose law? Is the lawfulness of the consent defined with reference to the Stored Communications Act itself? Or is it federal common law? Is it the law of the state the person is in?

MR. SNYDER: I believe it is lawful under the circumstances. So it would depend on what jurisdiction's law applies and the particular circumstances.

THE COURT: What position do you take to whose law applies to decide whether the consent is lawful? Is there a law of Stored Communications Act cases that decides whether consent is lawful?

MR. SNYDER: I mean, I believe that to the extent they're invoking California law, in this case we certainly believe that there was consent and authorization under California law. I'm not aware of a federal body of SCA consent law. But I think that in this case for sure --

(Pause.)

MR. LIPSHUTZ: I was going to say, Your Honor, that there are courts who have looked to Fourth Amendment jurisprudence to determine whether consent is appropriate, even in the SCA context, as well.

THE COURT: Might that be in the cases that you often

argue where law enforcement is trying to get its hands on the information?

MR. LIPSHUTZ: Law enforcement, or even a private criminal defendant through a subpoena. Those courts have often looked to Fourth Amendment jurisprudence to look at concepts of consent.

MR. SNYDER: But the one thing that's clear about the SCA in this case, Your Honor, taking it to --

THE COURT: That would be very much to Facebook's benefit if we were to look to Fourth Amendment law, I would assume. Because according to Fourth Amendment case law, defendants always consent.

MR. LIPSHUTZ: Well, Fourth Amendment case law incorporates the concept of third-party doctrines. Once you give up your information to a third party, that often is consent. Or, can be construed as consent for Fourth Amendment purposes.

THE COURT: So, I mean, that gets back to the question that I asked this morning about -- I mean, if we were using Fourth Amendment doctrine, which by the way I think is horribly dangerous to use Fourth Amendment doctrine in this context. But if we were to use it, we would say that the mere fact that I shared these communications with my friends reflects consent to disclose it to somebody else. Right?

MR. SNYDER: We're not arguing that, Your Honor. What

we're saying, though, in the facts of this case is that to look at the SCA you have to, under *Spokeo* and *Eichenberger*, go to the common law and see if there's a common law analog. And that's where the plaintiffs --

THE COURT: I'm not talking about standing. I'm talking about the merits. How to decide whether somebody gave consent to the disclosure of information.

MR. SNYDER: Well, consent under the -- here, we believe under California law is manifest. And if you look again at the *Smith* case decided in December of last year, the Ninth Circuit in affirming dismissal on the merits of a very similar argument made here that the consent didn't cover Facebook's data tracking and collection policies, the court affirmed the dismissal. And on basic, you know, black letter common law contract principles that you consider the circumstances and whether a reasonable person would read the disclosures to cover the conduct at issue.

And so I think it's a pretty straight forward analysis, both common sensical and straight forward. A person -- and it does go back elementally to what Your Honor referred to as sort of general propositions of law in our brief. Where we said, you know, consent, where clear and where on point, is dispositive of the question of whether you authorized an act or not.

And so I think that the disclosures here are crystal

clear. I understand Your Honor's going to give -- likely give -- or, going to give them a chance to amend. I don't think there's a way to amend this complaint as it relates to the disclosures that will cure what is a fatal defect. And again, it goes, Your Honor, to the complaint which Your Honor referred to --

THE COURT: Well, maybe one of the things they could do is respond to some of the points you've just made about the business partners. Which I think a lot of the points you made are not, you know, subject to judicial notice, probably. But, you know, maybe they would be able to beef up their allegations about the disclosure about what was shared and not shared with business partners, and disclosure and the effect that it does or doesn't have on the user.

MR. SNYDER: And don't bite me, but back to standing what's a another glaring omission in the complaint. Is none of the plaintiffs allege what he or she used to access Facebook, if anything, on a mobile device.

THE COURT: Mobile device? That's true. I think some of them alleged that they used Facebook on their phones and stuff like that.

MR. SNYDER: I don't believe they identified what device or what platform. And the fact is -- and, again, this isn't in the complaint -- but the fact is it may not be a mystery why. The Facebook-like experience was not a great

experience. It wasn't Facebook's platform. So some of these --

THE COURT: Well, at some point it was.

MR. SNYDER: It was. But in the early days, some of these operating platforms cobbled together the best Facebook they could create.

THE COURT: When did the Facebook app start appearing on the iPhone?

MR. SNYDER: It was on the iPhone -- that was the only other operating service it was on at the same time. But the others had to create their own experiences. And because they were so rudimentary, they weren't that popular, frankly. And so I wouldn't be surprised if the named plaintiffs had no experience or interaction with those operating systems.

THE COURT: Well, I mean, how long does the class period go to?

MR. SNYDER: I was asking me client what year Facebook was available on all other operating systems via the Facebook app. And we don't have that information at our fingertips. But I can tell you the complaint is silent as to all this. It just makes generic allegations about this in paragraph 271.

THE COURT: Could I suggest -- I want to -- I do want to talk about the Video Privacy Protection Act for a bit. Could I suggest that we take another break and come back at about quarter to 4 with an eye towards getting out of here like

no later than 4:30?

MR. SNYDER: Do you want to talk about the 12(b)(6) or 12(b)(1) video?

THE COURT: What do you think?

MR. SNYDER: 12(b)(6).

THE COURT: You got it.

MR. SNYDER: Is a thumbs up a purchase?

(Recess taken at 3:31 p.m.)

(Proceedings resumed at 3:53 p.m.)

THE COURT: Okay. Before we get to the Video Privacy Protection Act, is there any other burning issue that anybody wants to bring to my attention on the stuff we've talked about already?

Mr. Snyder is shaking his head: No, please, no more.

MR. LOESER: I don't know if it would be called a burning issue or just something that should be corrected.

And that's that Mr. Snyder went on at some length about how, particularly with regard to the business partners, the only sharing that occurred was with device makers. And based upon that, the disclosures were somehow adequate.

And first of all, even as to device makers, I don't think these disclosures come close. But more importantly what we learned after we filed the complaint, in the ***New York Times*** article, was that the disclosures were most assuredly not just to device makers.

THE COURT: What you learned after you filed this complaint?

MR. LOESER: We learned that on December 18, 2018. So we will come back to one of the wise suggestions Your Honor made about amendments. And I know one of the questions about what one would put in an amendment.

But I'm not quite sure where Mr. Snyder is getting his information. Maybe he saw the headline and didn't want to read the rest of the article. But the information also went to Spotify and Netflix and the Royal Bank of Canada and Qualcomm. And these are not device makers. These are a variety of companies that harvest information and use it. And the complaint alleges that they harvested Facebook information.

THE COURT: Now I assume what it is if you want to sign on to Spotify, for example, through Facebook, then they have some sort of business partnership where users are able to sign on to Spotify through Facebook. And in that way? Or would that be an example of sharing with an app?

MR. LOESER: That may be what they're doing. Unfortunately, since they didn't describe it in any of the disclosures, you know, we're relying on what the *New York Times* says they are doing.

And one thing just that's also worth mentioning, I do think it would be valuable for Your Honor to look at the current disclosures, what they're saying after all this scandal

and all these acknowledgments of not being entirely transparent.

THE COURT: Like as an example of how could you do it more clearly and less ambiguously?

MR. LOESER: Precisely. We've even made some helpful suggestions in our materials if you look at slides 3 through 6. These are just -- if Facebook wanted to clearly say what they were doing, they could make a clear disclosure. They could put it in the one place where all disclosures are made; which they've come much closer to doing now. And, again, that's --

This would be useful wouldn't it? This would make it pretty clear. Like the first one --

THE COURT: Well, that's not true. I mean, if they gave -- I'm looking at the one about business partners. It says: Facebook shares your content and information with Facebook's business partners without notice to you and without identifying the business partners.

I mean, that's not true, because this would give them notice that they're doing it.

MR. LOESER: Well, no. If they wanted to describe what they did -- I guess I should clarify. The disclosures in effect --

THE COURT: It's hard to do a disclosure.

MR. LOESER: These are not new. You're right. That's a very good point, Your Honor. These are -- when we try and

understand what happened, and we allege the facts we've alleged based on the information that's available, what's happened is what these statements say: Facebook shares your content and information with Facebook business partners without notice to you and without identifying the business partners.

That would be a really useful thing for someone to know. And it might be one of those things that would cause you to look at your settings differently; to go back to an earlier point. So I think that's --

THE COURT: Could I ask you one other question just -- when you showed me that, this other slide caught my eye. The one that you showed me before that you've titled "Facebook's Empty Apologies" and you quote people from Facebook saying: It was a breach of trust. And: We're sorry.

Did you include in the complaint any contemporaneous statements by Facebook officials about the degree to which people's privacy is protected?

MR. LOESER: I believe so. I think we've included everything we could find in any article that -- you know, we pretty scrupulously tried to pull all --

THE COURT: I mean, statements that were made during the class period before the quote-unquote empty apologies.

MR. LOESER: Privacy is so important to us. We always protect it. We never sell data.

Selling data, by the way, the best description I've heard

as to why that statement is wrong was from a Stanford business professor who likened Facebook's statement, they never sell data, to a bar giving away martinis with $12 bags of peanuts and telling people that they don't sell drinks.

Selling data and selling access to data -- for the life of me I can't figure out the difference is between those two things.

So we've collected statements like that particularly about the privacy and the importance of it and what they've done to protect it. And we've also cataloged, with every scandal that's happened, what executives have said about that.

MS. WEAVER: The statement about during the class period begin at paragraphs 344. And it's -- for example, CEO Zuckerberg writing in an op-ed: The principles under which Facebook operates, you have control over how your information is shared. We do not share your personal information with people or services you want. We do not give advertisers access to your personal information. We do not, and never will, sell any of your information to anyone.

And I wanted to make one clarifying point right on that issue, as well. And, Your Honor, might have caught it. But when Mr. Snyder was speaking at paragraph 275. Right at the end of the disclosure -- it's at the top of page 105 in the complaint -- it has that sentence again: The application will be allowed to use that information only in connection with the

person that gave the permission and no one else.

But, of course, Cambridge Analytica -- Kogan sold the data to Cambridge Analytica. You might have even said that, Your Honor, at the time.

THE COURT: But that's more -- that's not about the disclosure of private information. It's about how the information is then used by the people to whom it was disclosed. So, for example, the Stored Communications Act, I mean, you don't have any claim under the Stored Communications Act based on how the information was later used by the people to whom it was disclosed.

MS. WEAVER: I think that's our negligence claim, among others. But -- unfair business practices. Because they know -- and we do have very specific allegations. For example, at paragraph --

THE COURT: What about your privacy claims? Does that language relate to your common law privacy claims?

MS. WEAVER: I would think so. Because it has to do with whether you had a reasonable expectation of privacy. They told you they did. CEO Zuckerberg did. Those paragraphs that you were asking about go directly to that. And, in fact, they weren't auditing. And there were allegations at paragraph 313 through 326. Here at paragraph 157, Dr. Kogan finally broke his silence in an interview with CBS News. He explained that the ability to gather people's Facebook friends' data without

their permission was a core feature available to anyone who was a developer.

THE COURT: I mean --

MS. WEAVER: He said Facebook never --

THE COURT: I don't know how valuable Kogan's statements are in that regard.

MS. WEAVER: Well, I mean, his terms of service, which we also reference here, flat out said that they would be selling information. And Facebook's response on that is that it claims not to have read them. I think they disagree. But there were other apps that were also selling data at the time.

And in any event -- so what we have, just to repeat, is Mr. Snyder made a factual representation that is in contradiction of our complaint. We have reasons for pleading it. And if the judge is going to make credibility decisions, it seems like that's more for summary judgment than just --

THE COURT: Credibility decision, it's not even for summary judgment. It's for trial.

MS. WEAVER: Fair enough.

THE COURT: On the Video Privacy Protection Act -- is that what it's called?

MS. WEAVER: Yes.

MR. SNYDER: Am I standing yet?

THE COURT: If you're arguing about this, yeah.

I guess -- so where is the definition of videotape service

provider? Here it is: Any person engaged in the business of rental, sale, or delivery of similar audiovisual materials.

MR. SNYDER: Correct.

THE COURT: So Facebook is -- I guess Facebook is not engaged in the delivery of audio visual materials?

MR. SNYDER: Facebook is not in the business of the rental, sale or delivery of videos in the manner that Congress intended to cover by the VPPA. That's correct. What Facebook does is it allows friends to share --

THE COURT: But just using the plain language of the statute.

MR. SNYDER: Yes.

THE COURT: Engaged in the business of delivery of audiovisual materials.

MR. SNYDER: I understand the language.

THE COURT: Facebook does not deliver audiovisual materials through its service?

MR. SNYDER: Not as that word has its plain meaning in the context of this statute. If you take the word "deliver," isolated from everything else, it can have a myriad of meanings. Within the context of this statute, it means delivery for the purpose of purchase, sale, a transaction. If you look at the legislative history it's clear -- I could cite Your Honor to it.

THE COURT: No. I mean, it's rental, sale or

delivery. But something other -- "delivery" means something other than rental or sale.

MR. SNYDER: "Delivery" for the purpose of a specific transaction. And if you look at the Senate report, it prohibits disclosure of, quote, "information that identifies a particular person as having engaged in a specific transaction," which is why every single VPPA case has involved the illegal disclosure of record of a video transaction itself, whether it's Hulu, Netflix in the modern age, or Blockbuster in the olden days. And that's because this statute, again, is prescribing the so-called Bork statute. All right?

The disclosure of personally identifiable information, which we don't have here. So the first point is Facebook is not a videotape service provider. It does not sell, rent or deliver for the purpose of a transaction, of the kind contemplated by the statute, video services. It also --

THE COURT: Well, but so -- so I gather what you're saying is Facebook -- there is never any -- there's never any purchasing of videos that takes place on Facebook?

MR. SNYDER: As alleged in the complaint and as relates to this case, absolutely not.

THE COURT: Okay.

MR. SNYDER: Absolutely not.

THE COURT: So there's no allegation -- let me pull up the complaint.

MR. SNYDER: The allegations here are that -- they're really twofold. Two arguments, Your Honor. After you get past the videotape service provider, they say it's been interpreted broadly to include companies offering streaming video services like Hulu. And it's true that modern versions of selling and renting videos is covered, for sure. But Hulu, which exclusively provides video services, Facebook's core services have nothing to do with the rental, sale or delivery of audiovisual materials. And so the VPA doesn't apply to disclosures unrelated to those kinds of transactions.

So --

THE COURT: Let me ask you to -- let me give you a hypothetical case.

MR. SNYDER: Sure.

THE COURT: Let's say like TaskRabbit. You know TaskRabbit? Probably one of your clients? No?

MR. SNYDER: Love TaskRabbit.

THE COURT: You love TaskRabbit? Okay. I don't know if this is true of TaskRabbit, but let's say you can go on TaskRabbit and you can get people to bring you stuff from various stores. So let's say -- let's just say you're able to go on TaskRabbit and send somebody to Target to buy you a bunch of stuff, including, you know, Al Gore's *An Inconvenient Truth* and Michael Moore's *Bowling For Columbine* and Robert Reich's *Aftershock*.

And the TaskRabbit people have a record of you having ordered that online through them, and they deliver it to you. And any time you ask to buy a video at Target, or whatever, they bring you a video. And then let's say that TaskRabbit discloses that you ordered all of those left wing videos through them.

Is that not --

MR. SNYDER: I believe that would be, because it would reflect a sale or a transaction. In fact --

THE COURT: So even though TaskRabbit wasn't --

MR. SNYDER: The Senate report deals with that, Your Honor. Senate report number 100-599, at page 12. And they talk about a department store, which I guess is not TaskRabbit, but it's a close relative.

A department store that sells videotapes would be required to extend privacy protection to only those transactions involving the purchase of videotapes, and not other products. And so simply because a business is engaged in the sale of rental or video materials doesn't mean that all its products or services are within the scope of the bill.

THE COURT: But if Facebook --

MR. SNYDER: Whether they be a videotape service provider would be a separate question.

THE COURT: Why wouldn't they be?

MR. SNYDER: Because they're not engaged in that

business. So I don't know --

THE COURT: I don't understand why that matters. If TaskRabbit disclosed the video watching habits of Robert Bork and his family, compared to Blockbuster disclosing it, why would that matter from Congress's standpoint given the protection that they were seeking to confer on?

MR. SNYDER: Because what Facebook does as a platform is not the delivery of video cassettes in connection with, in the aftermath of, or as a result of a specific transaction.

THE COURT: Well, it doesn't have to be video cassettes.

MR. SNYDER: Video. Video. I meant video.

THE COURT: But I'm asking about TaskRabbit right now. Is TaskRabbit --

MR. SNYDER: If they're facilitating the sale or transaction, and have a record of personally identifiable information within the meaning of the statute, arguably yes. But we don't have that fact pattern here because Facebook is not delivering, in any manner, videos.

THE COURT: Does Facebook facilitate the delivery of video from one person to another?

MR. SNYDER: It allows a friend to share videos on the Facebook platform for sure, but not for the purpose of a sale or rental or a transaction. And it's very clear from the legislative history that the VPPA doesn't prohibit the sharing

-- only prohibits disclosure of, quote, "information that identifies a particular person as having engaged in a specific transaction."

And where the complaint fails here, and there is no way to cure it, is that there was no sale or rental or transaction of a video in connection with the events alleged in the complaint.

What they allege is two things. They allege that there was "likes" of videos, and that people were tagged in videos. Neither is a transaction even remotely within the contemplation of Congress. And Facebook hasn't disclosed records of a single transaction to request or obtain videotape services.

If a user is tagged, that's not personally identifiable information, because a tag is simply a statement that a user is in the video; not that she's requested it, or obtained it, bought it, sold it. And tagging doesn't even indicate any action at all by the user. A user is tagged oftentimes by the friend who's posting it.

A user who likes a video, that's not personally identifiable information, either, under the Act. Because all that means is that a user's connected to a Facebook page and they have indicated that they like it. It is not a transaction. There's no request to obtain any video.

And, finally, any videos in a user's news feed, which is a way that you can be served videos, is not personally identifiable information because Facebook determines what

content appears there. And the fact that a video was in a user's news feed certainly does not identify the user has requested, much less bought or rented, much less even viewed the video.

So this statute is a -- not applicable to any of the facts in this case. And if you look at the clear legislative history, and every single case that's involved the VPPA, has involved the alleged disclosure of a record of a video transaction itself. Including the, going back to the ***Eichenberger*** case -- I'm not going to talk about standing -- where, of course, they found no claim because they determined that there wasn't personally identifiable information for a different reason.

And so none of the video-related content that the plaintiff here alleges was shared meets the definition of personally identifiable information. And they would have to allege, which they couldn't, that a user requested or obtained video materials in a specific transaction, which is not this case at all.

So it really is a statute that's far afield of these cases. I like your TaskRabbit example because it is an actor in the chain of a video transaction itself, which we don't have present here.

THE COURT: If I were uncomfortable reading the word "delivery" out of the statute -- in other words, which seems to

be what you're trying to do. You said has to be -- or, to the extent that delivery involves, it has to be delivery in connection with a sale or rental.

MR. SNYDER: A transaction, I would say, yes.

THE COURT: Then what's your definition of a transaction?

MR. SNYDER: I mean, I guess you can rent or buy --

THE COURT: If I send -- if I email a video to you, isn't that -- like let's say --

MR. SNYDER: A subscription. Yeah, it can be a subscription service.

THE COURT: Over gmail if I delivered a video to you, aren't I delivering the email to you? I mean -- excuse me -- the video to you?

MR. SNYDER: You are within the ordinary plain meaning of the word "delivery." But, of course, statutory construction requires that you read words in a statute in a context of all the words used and the entire statute. And then, of course, the legislative history. And when you do that, there's no fair reading of this statute that would apply to liking or tagging videos or watching videos in your news feed which are the only categories of information regarding videos that the plaintiffs here allege was shared.

I'll just note that the Ninth Circuit has indicated --

THE COURT: Yeah, yeah. I know. I know. In dicta.

MR. SNYDER: In dicta. But I think they read the statute and --

THE COURT: I understand. And Judge Seeborg did it, too, in a case.

But does Facebook engage in -- I guess the -- you know, the first answer to my question is going to be that's not in the complaint.

MR. SNYDER: Correct.

THE COURT: But does Facebook advertise any services, you know, related to the sharing of videos or the delivery of videos? Like: Hey, here's what you can do with videos on Facebook.

MR. SNYDER: Not that I'm aware of, Your Honor.

THE COURT: Here's how you can show videos to your friends on Facebook. Here's how you produce them and here's --

MR. SNYDER: I don't believe so. I imagine there are basic instructions for sharing photos and everything else that facilitates the social experience of Facebook. But there's nothing that I'm aware of that instructs people how to sell videos or enter into transactions.

THE COURT: Or promote themselves with videos or promote their --

MR. SNYDER: No. And the statute, really, is clear if you read the legislative history.

THE COURT: If there were, would it matter?

MR. SNYDER: No. There needs to be, Your Honor, a specific transaction. That's what the Senate report makes clear and that's what the statute itself makes clear. Because the definition of personally identifiable information in the Senate report is, quote, "intended to be transaction oriented." And then, quote, "limited to," quote, "information that identifies a particular person as having engaged in a specific transaction."

And we just don't have transactions. We have the viewing -- maybe the viewing of videos. We don't even know that because we know that when someone likes a video they could have watched it, they could not have watched it. And so there is no transaction here and there is no --

THE COURT: Okay. Other.

MR. SNYDER: -- really plausible allegation that the statute is implicated, much less violated.

THE COURT: Okay.

MR. SNYDER: Thank you.

THE COURT: Plaintiffs want to talk about that?

MS. WEAVER: Yes, please. Thank you, Your Honor. We'll be brief.

I think on its face the statute says: The rental, sale or delivery of pre-recorded video cassette tapes. The Merriam Webster Dictionary of "delivery" is: Send, provide, or make accessible to someone electronically.

We allege in multiple paragraphs, including 71, 73, 83 that plaintiffs watched videos. In paragraph 126 of the complaint -- I'll read to you. It's talking about Graph API, Version 1, which is Facebook's platform. It says: Developers could ask Facebook's permission to access further categories of information. Video information was also available to developers through at least seven different categories of data.

Paragraph 126 says: The data queries user's video and friend's video permissions allowed app developers to obtain the videos the user has uploaded, et cetera.

The question of legislative history wasn't raised until defendant's reply brief, but I'm happy to address it. *In Re*: *Vizio* at 238 F.Supp.3d --

THE COURT: Can I -- I'm happy for you -- well, go ahead and finish that, then I have a question. Sorry to interrupt.

MS. WEAVER: Okay. No, no. *Vizio* expressly says: The plain text of the statute provides otherwise. As an initial matter, Congress's use of a disjunctive list, i.e., engaged in the business of sale or delivery, unmistakably indicates that Congress intended to cover more than just the local video rental store. Indeed, lest the word "delivery" be superfluous, a person need not be in the business of either renting or selling video content for the statute to apply.

THE COURT: That doesn't directly contradict the point

that there has to be a transaction even if the person themselves is not doing the selling or renting. But I understand your point.

I guess one problem is from reading -- you know, I asked this question about does Facebook advertise how videos can be used on Facebook and stuff like that. I don't know the answer to any of those questions. But I was left reading claim 2 of the complaint with kind of a foggy picture of how videos are used on Facebook.

MS. WEAVER: Okay.

THE COURT: And so, you know, there are -- you know, you kind of go straight to -- you say: Facebook is a videotape service provider because Facebook regularly displays a variety of video content to its users. And it says: Plaintiffs and the other class members are consumers because they are subscribers of goods or services from Facebook videotape service provider.

I'm not actually sure -- you didn't argue this, but I'm not actually sure they are consumers within meaning of the statute. But that wasn't argued.

And then you go on to talk about the kind of information that was obtained as a result of, you know, peoples' activities on Facebook relating to videos. But I was left with sort of a foggy picture about what are the kinds of things that people, you know, do with videos, and what are the kinds of services

that Facebook provides vis-à-vis videos.

And maybe this is a product of my not having been on Facebook since I learned I would be nominated to the bench. And, you know, I think Facebook has evolved quite a bit since that time with probably, in particular, with respect to video.

And there's nothing in the complaint that helps me really understand it. So I wonder if that's another issue.

MS. WEAVER: Sure. Paragraph 73 it says: Plaintiff Schinder has watched and liked videos on Facebook and has also liked pages on Facebook that contain videos.

Mr. Snyder explained to you --

THE COURT: But in terms of like -- you're hinging your argument on the word "delivery," right?

MS. WEAVER: Yes.

THE COURT: And maybe it's obvious and I'm just not -- maybe I'm the only one it's not obvious to. But what is the delivery that happens? That's what -- I was hoping for an explanation in the complaint about what Facebook does with respect to videos and how it constitutes delivery within the meaning of the statute.

MS. WEAVER: Okay. The allegations at 125 through 129 address videos. And if you look at 129, this is the interaction between Facebook and app developers. And I think you're asking how the users get the videos first. But --

THE COURT: Yeah. I wasn't asking about information

that apps get.

MS. WEAVER: But this is relevant, too. Your first question is: I don't know the technicalities. The Facebooks (sic) are on Facebook site. The users access them on Facebook site. The definition of "delivery" is make accessible to someone electronically. Facebook is doing that. I don't know how and I don't know the specifics. I'm not an engineer. But anybody who's on Facebook can look on -- well, watch videos, send them to people, like them, share them, post them, et cetera. And we don't allege that they just tag them or just did a "like." We say they watched them.

THE COURT: And do you say that the apps get information about whether the user watched the video?

MS. WEAVER: They have -- that's -- so, for example, Facebook allowed app developers access to video information through the read/stream query. The developer web page defined this category as providing access to all the posts. This information would include any videos uploaded by the user, as well as any videos or video hyperlinks shared with the user.

And I would just note the statute doesn't cover whether or not the user watched it, so that's not a requirement. I don't know that necessarily the apps know whether or not they watched them or not.

With regard to Mr. Bork --

THE COURT: But if they know that you uploaded it. I

mean, that's a significant thing. Right?

MS. WEAVER: Yes.

THE COURT: I kind of understand the point that just because you liked -- somebody else posts a video and you say that you liked it doesn't necessarily mean that you watched it. Right?

MS. WEAVER: Right. But that just ignores what we pled. We pled people watched them. They have specific plaintiffs with standing here saying they watched the videos that fall within the definition of --

THE COURT: Well, no. But the point is that there has to be -- I think what's missing is what information did the apps get? You're saying the apps did get information that people downloaded videos, which I think is probably close enough to watching.

But then how does the delivery of videos work on Facebook? There's -- you know, there's a little bit missing there.

Anyway, Mr. Snyder, you don't need to get up again if you don't want to --

MS. WEAVER: Just to be clear, the term "consumer" in the statute is any renter, purchaser or subscriber of goods or services. So they don't have to have watched it. They just have to have received it.

THE COURT: Okay. Real quick question for Mr. Snyder.

What about YouTube? On your definition it sounds like

YouTube would not be covered by this statute.

MR. SNYDER: It depends whether it's a subscription or whether there's a sale or free watching.

THE COURT: So if I go on YouTube and I watch a video, and YouTube keeps track of all the videos I watch and then discloses to the world all of the videos that I've watched, it's not covered by this statute?

MR. SNYDER: You know, I don't know enough about how YouTube serves its videos. The answer is YouTube is in the video business.

THE COURT: There's no transaction.

MR. SNYDER: Deliver within the -- meaning of the word "delivery" given legislative intent of the statute. I'd have to think about that. But they may have immunity unless Congress amends the statute to make clear that it covers those kinds of services as opposed to transactions.

THE COURT: Okay.

MR. SNYDER: But luckily, we don't have those facts.

THE COURT: YouTube is not your client?

MR. SNYDER: Not my client.

THE COURT: Okay. I think this is my last question. We talked about -- you know, we've now been here for like five hours or six hours, or something like that. You know, I think we've talked about a number of potential problems with the complaint. I talked to you -- introduced this concept to you

earlier. And so let me just ask you now given this discussion. Do you believe you've taken your best shot at alleging standing? And, you know, stating claims under the various causes of action that you've asserted?

MR. LOESER: Here's how I think I can answer that question, Your Honor. We believe the complaint sufficiently satisfies standing and satisfies 12(b)(6); however, we will take the invitation to introduce a host of additional facts, some of which we discussed today, most of which became available after we filed our complaint. So it's really, I guess, a question for you. Would you like us to file an amended complaint based upon an order in which you've provided some limitation or expanded the theories we can pursue? Or should we just filed amended complaint?

THE COURT: I think you have a transcript of a six-hour hearing. And, you know, like I said, I think there's -- I think district court's general practice should be to, in complicated cases like this, to not do multiple lengthy opinions. I don't think it advances the case in any way. In fact, it slows the case down because everyone's sitting around waiting for an opinion.

And, you know, on the first round of a motion to dismiss like this everybody has a lot of food for thought now. And if we took this route of simply giving you -- you know, giving you leave to amend right now, file an amended complaint, I would

assume that the next iteration of it would be your best shot. And that absent some extraordinary circumstances, if a particular claim is inadequate, it would be dismissed with prejudice.

MR. LOESER: Understood, Your Honor. And we will take you up on what I think is an offer.

I do think it's important, even in that context, to say if you step back and look at what's been disclosed about Facebook, what scandals have been unearthed, what Facebook executives have been saying about it; and then you put together the allegations that we base on that, we've taken a lot of information that Facebook didn't volunteer, most of which was disclosed through reporting and other things.

And there is an asymmetry in the information at the beginning of a case. And I do think that's why at the motion to dismiss stage it's appropriate to draw inferences in the plaintiffs' favor and why factual disputes get decided at a later stage.

So we will take you up on the idea. I think it's a good idea. I think that there's no sense having two orders. And we will add all the facts that we can, and hopefully it's sufficient on all the claims.

THE COURT: And, you know, one benefit of doing it this way is, you know -- when did you all file this case?

MS. WEAVER: September.

THE COURT: You can have 21 days to amend your complaint. We'll have another motion to dismiss, I assume, unless Facebook reads the amended complaint and decides there's standing and the claim has been stated. And we can have a hearing on it, and well before a year you'll have a ruling on whether you have a case or not. Which I think is sort of an efficient way of handling the case in the trial court.

MR. LOESER: I think that would be appropriate. I think we, obviously, strongly believe that it's time for Facebook to respond to some discovery so that all of these factual issues can really be put to rest. And we look forward to the opportunity to do that.

THE COURT: Okay. Any final comments?

MR. SNYDER: The comment, obviously, is we trust Your Honor's judgment about how best to efficiently handle the case, so we're fine with that procedure.

With two points. One, you know, we're going to reserve the right to object if they try to enlarge their pleading beyond the theories in the second amended complaint. We think they should stay within the scope of the existing complaint. And then the second is, as Your Honor observed last time when they tried to get discovery, we don't believe that they should use this opportunity to try to get discovery because that's all backwards. I mean, I think we've given them a road map and --

THE COURT: I was operating under the assumption that

there would be no further -- I mean, I did allow some discovery, but there would be no further discovery until the next hearing on the next possible motion to dismiss.

MR. SNYDER: And then the final point is even with the extensive roadmap that they now have, we believe that amendment here would be futile. But we look forward to seeing the pleading and I would be shocked if we didn't file another motion to dismiss, because we don't believe that any allegations they can make in good faith will give rise to standing or any actionable claims here.

THE COURT: Why don't we plan -- why don't we give the plaintiffs 21 days from today to file an amended complaint. And why don't you all work together on your schedules and stuff and we'll plan on having a hearing.

What is it? We're in early February now, so why don't we have a hearing in May. Why don't you set it up so that we have a hearing in May.

MR. SNYDER: I agree.

MR. LOESER: Your Honor, just in interest of avoiding needless dispute. When counsel says "the right to object to expanding the pleadings --"

THE COURT: And you have the right to respond to the objection.

MR. LOESER: Well, I just want to make clear what we have in mind to do is to add a lot more facts. We don't have

in mind to add additional claims. So I take it that counsel isn't objecting to the addition of new factual material.

THE COURT: I'm sure they'll object to everything, but we can worry about that later.

MR. LOESER: Okay. Thank you, Your Honor.

THE COURT: All right. Thank you.

---oOo---

CERTIFICATE OF REPORTER

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

DATE: Monday, February 4, 2019

Vicki Eastvold, RMR, CRR
U.S. Court Reporter